



Hewlett Packard
Enterprise

HPE MSR1000_MSR2000_MSR3000_MSR4000_ MSR9XX-CMW710-R6749P14 Release Notes

Contents

Version information	1
Version number	1
Version history	2
Hardware and software compatibility matrix	4
Upgrade advice	6
Upgrading restrictions and guidelines	7
Hardware feature updates	7
CMW710-R6749P14	7
CMW710-R6728P25	7
CMW710-R6728P20	7
CMW710-R6728P15	7
CMW710-R0821P11	7
CMW710-R0809P33	7
CMW710-R0809P32	8
CMW710-R0809P29	8
CMW710-R0809P27	8
CMW710-R0707P24	8
CMW710-R0707P21	8
CMW710-R0707P19	8
CMW710-R0707P16	8
CMW710-R0707P12	8
Software feature and command updates	8
MIB updates	9
Operation changes	10
Restrictions and cautions	10
Open problems and workarounds	10
List of resolved problems	11
Resolved problems in CMW710-R6749P14	11
Resolved problems in CMW710-R6728P25	11
Resolved problems in CMW710-R6728P20	12
Resolved problems in CMW710-R6728P15	13
Resolved problems in CMW710-R0821P11	13
Resolved problems in CMW710-R0809P33	14
Resolved problems in CMW710-R0809P32	14
Resolved problems in CMW710-R0809P29	14
Resolved problems in CMW710-R0809P27	15
Resolved problems in CMW710-R0707P24	16
Resolved problems in CMW710-R0707P21	17
Resolved problems in CMW710-R0707P19	18
Resolved problems in CMW710-R0707P16	18
Resolved problems in CMW710-R0707P12	19
Support and other resources	19
Accessing Hewlett Packard Enterprise Support	19
Documents	20
Related documents	20
Documentation feedback	21
Appendix A Feature list	22
Hardware features	22

Software features	32
Appendix B Upgrading software	36
Software types	36
Upgrade methods	36
Preparing for the upgrade	37
Centralized devices upgrading from the CLI	38
Saving the running configuration and verifying the storage space	38
Downloading the image file to the router	39
Specifying the startup image file	40
Rebooting and completing the upgrade	41
Distributed devices upgrading from the CLI	42
Display the slot number of the active MPU	42
Save the current configuration and verify the storage space	43
Download the image file to the router	43
Specifying the startup image file	44
Reboot and completing the upgrade	46
Distributed devices ISSU	47
Disabling the standby MPU auto-update function	48
Saving the running configuration and verifying the storage space	48
Downloading the upgrade image file to the router	49
Upgrading the standby MPU	50
Upgrading the active MPU	51
Upgrading from the BootWare menu	53
Accessing the BootWare menu	53
Using TFTP/FTP to upgrade software through an Ethernet port	55
Using XMODEM to upgrade software through the console port	58
Managing files from the BootWare menu	63
Displaying all files	64
Changing the type of a system software image	64
Deleting files	65
Handling software upgrade failures	66
Appendix C Handling console login password loss	66
Disabling password recovery capability	66
Handling console login password loss	67
Examining the password recovery capability setting	68
Using the Skip Current System Configuration option	69
Using the Skip Authentication for Console Login option	70
Using the Restore to Factory Default Configuration option	70

List of Tables

Table 1 Version history.....	2
Table 2 MSR1000/MSR2000/MSR3000/MSR4000 product device numbers matrix	4
Table 3 MSR1000/MSR2000/MSR3000/MSR4000 Hardware and software compatibility matrix.....	5
Table 4 MIB updates	9
Table 5 MSR1000 specifications	22
Table 6 MSR2000/MSR2000 TAA specifications	22
Table 7 MSR3000/MSR3000 TAA specifications	23
Table 8 MSR4000 specifications.....	24
Table 9 MSR4000/MSR4000 TAA MPU Specification.....	24
Table 10 MSR4000 SPU Specification	24
Table 11 MSR2004-24 AC power module specifications.....	25
Table 12 MSR2004-48 DC power module specifications	25
Table 13 MSR3044/MSR3064/MSR4060/MSR4080 AC power module specifications	25
Table 14 MSR3044/MSR3064/MSR4060/MSR4080 DC power module specifications.....	25
Table 15 MSR3044/MSR3064/MSR4060/MSR4080 PoE power module specifications	25
Table 16 MSR954P_MSR958 specifications.....	25
Table 17 MSR954 specifications.....	26
Table 18 MSR1002X 4 technical specifications.....	26
Table 19 MSR30X6/MSR30X8 TAA specifications	27
Table 20 MSR954-V2specifications	28
Table 21 MSR series routes Module List	28
Table 22 Sierra Modem Module and Host/card compatibility matrix.....	32
Table 23 MSR Series routers software features.....	32
Table 24 Storage media	37
Table 25 BootWare menu options.....	55
Table 26 Ethernet submenu options	55
Table 27 Network parameter fields and shortcut keys.....	56
Table 28 Serial submenu options	58
Table 29 File Control submenu options	64
Table 30 BootWare options and password recovery capability compatibility matrix	66

This document describes the features, restrictions and guidelines, open problems, and workarounds for version R6749P14. Before you use this version in a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with HPE
MSR1000_MSR2000_MSR3000_MSR4000_MSR9XX-CMW710-R6749P14 Release Notes
(Software Feature Changes) and the documents listed in [“Related documents”](#)

Version information

Version number

HPE Comware Software, Version 7.1.064, Release 6749P14

Please see the example below generated by the display version command:

```
<HPE> display version
HPE Comware Software, Version 7.1.064, Release 6749P14
Copyright (c) 2010-2022 Hewlett Packard Enterprise Development LP
HPE MSR3012 uptime is 0 weeks, 5 days, 3 hours, 16 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr3000-cmw710-boot-r6749P14.bin
Boot image version: 7.1.064P80, Release 6749P14
  Compiled Jun 16 2022 15:00:00
System image: cfa0:/msr3000-cmw710-system-r6749P14.bin
System image version: 7.1.064, Release 6749P14
  Compiled Jun 16 2022 15:00:00
Feature image(s) list:
  cfa0:/msr3000-cmw710-data-r6749P14.bin, version: 7.1.064
    Compiled Jun 16 2022 15:00:00
```

Slot 1: HPE MSR3012 uptime is 0 weeks, 5 days, 3 hours, 16 minutes

Last reboot reason : User reboot

CPU ID: 0x2

1G bytes DDR3 SDRAM Memory

8M bytes Flash Memory

PCB Version: 2.0

CPLD Version: 2.0

Basic BootWare Version: 1.82

Extended BootWare Version: 1.82

[SUBSLOT 0]AUX	(Hardware)2.0,	(Driver)1.0,	(CPLD)2.0
[SUBSLOT 0]GE0/0	(Hardware)2.0,	(Driver)1.0,	(CPLD)2.0
[SUBSLOT 0]GE0/1	(Hardware)2.0,	(Driver)1.0,	(CPLD)2.0
[SUBSLOT 0]GE0/2	(Hardware)2.0,	(Driver)1.0,	(CPLD)2.0
[SUBSLOT 0]CELLULAR0/0	(Hardware)2.0,	(Driver)1.0,	(CPLD)2.0
[SUBSLOT 0]CELLULAR0/1	(Hardware)2.0,	(Driver)1.0,	(CPLD)2.0
[SUBSLOT 3]HMIM-8GSW	(Hardware)3.0,	(Driver)1.0,	(CPLD)1.0

Version history

For information about version R0707P24 and earlier for MSR954_MSR954P_MSR958 series routers, see *HPE MSR954_MSR954P_MSR958-CMW710-R0707P24 Release Notes*.

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
CMW710-R6749 P14	CMW710-R6728P25	2023-06-28	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series and MSR1002X 4 - New Hardware feature Add new hardware: S0W32A (HPE MSR 4p Gig-T HMIM-V2 Mod) S0W33A (HPE MSR 8p Gig-T HMIM-V2 Mod) S0W34A (HPE MSR 8p 1000BASE-X HMIM-V2 Mod) S0W35A (HPE MSR 16p Enh Async Serial HMIM-V2 Mod) S0W31A (HPE MSR954-V2 1GbE SFP Router) - New Software feature - Modified Software feature:
CMW710-R6728 P25	CMW710-R6728P20	2022-12-08	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series and MSR1002X 4 Fixes bugs
CMW710-R6728 P20	CMW710-R0821P15	2022-06-23	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series Fixes bugs
CMW710-R6728 P18	None	2022-05-28	Release version	MSR1002X 4 first Release
CMW710-R6728 P15	CMW710-R0821P11	2022-01-25	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series - New Hardware feature Add new hardware: RT-SIC-4GSWF - Fixes bugs
				MSR30X6_MSR30X8 first Release
CMW710-R0821 P11	CMW710-R0809P33	2021-03-19	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958

				series Fixes bugs
CMW710-R0809 P33	CMW710-R0809P32	2020-12-15	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series Fixes bugs
CMW710-R0809 P32	CMW710-R0809P29	2020-11-12	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series Fixes bugs
CMW710-R0809 P29	CMW710-R0809P27	2020-08-10	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series - Modified feature: - Configuring an IPv6 static route - Fixes bugs
CMW710-R0809 P27	CMW710-R0707P24	2020-06-29	Release version	MSR1000_2000_3000_4000_series and MSR954_MSR954P_MSR958 series - New feature: - Configuring the DHCP-designated default router as the next hop of a static route - Applying an SSL server policy to the RESTful access over HTTPS service - Applying an SSL server policy to the NETCONF over SOAP over HTTPS service - Fixes bugs
CMW710-R0707 P24	CMW710-R0707P21	2020-03-25	Release version	MSR1000_2000_3000_4000 series, including MSR1003-8S - Modified feature: - Processing for user IP conflicts on an LNS - Login password control - Fixes bugs
CMW710-R0707 P21	CMW710-R0707P19	2019-11-07	Release version	MSR1000_2000_3000_4000 series, including MSR1003-8S Fixes bugs
CMW710-R0707 P19	CMW710-R0707P16	2019-09-20	Release version	MSR1000_2000_3000_4000 series, including MSR1003-8S Fixes bugs
CMW710-R0707 P16	CMW710-R0707P12	2019-06-20	Release version	MSR1000_2000_3000_4000 series, including MSR1003-8S - Modified feature: Ethernet interface - Fixes bugs
CMW710-R0707 P12	CMW710-R0615P16	2019-03-16	Release version	MSR1000_2000_3000_4000 series, including MSR1003-8S - New feature: - RADIUS ACL assignment by ACL

				name
				Fixes bugs.

Hardware and software compatibility matrix



CAUTION:

To avoid an upgrade failure, use [Table 3](#) to verify the hardware and software compatibility before performing an upgrade.

Table 2 MSR1000/MSR2000/MSR3000/MSR4000 product device numbers matrix

Product code	HPE Product name
JG402A	HPE MSR4080 Router Chassis
JG403A	HPE MSR4060 Router Chassis
JG404A	HPE MSR3064 Router
JG405A	HPE MSR3044 Router
JG406A	HPE MSR3024 AC Router
JG407A	HPE MSR3024 DC Router
JG408A	HPE MSR3024 PoE Router
JG409A	HPE MSR3012 AC Router
JG410A	HPE MSR3012 DC Router
JG411A	HPE MSR2003 AC Router
JG412A	HPE MSR4000 MPU-100 Main Processing Unit
JG413A	HPE MSR4000 SPU-100 Service Processing Unit
JG414A	HPE MSR4000 SPU-200 Service Processing Unit
JG670A	HPE MSR4000 SPU-300 Service Processing Unit
JG875A	HPE MSR1002-4 AC Router
JH060A	HPE MSR1003-8S AC Router
JG861A	HPE MSR3024 TAA-compliant AC Router
JG734A	HPE MSR2004-24 AC Router
JG735A	HPE MSR2004-48 Router
JG866A	HPE MSR2003 TAA-compliant AC Router
JG869A	HPE MSR4000 TAA-compliant MPU-100 Engine
JG409B	HPE MSR3012 AC Router
JH373A	HPE MSR954 Serial 1GbE Dual 4GLTE (WW) CWv7 Router
JH300A	HPE MSR958 1GbE Combo 2GbE-WAN 8GbE-LAN CWv7 Router
JH301A	HPE MSR958 1GbE Combo PoE+ 2GbE-WAN 8GbE-LAN CWv7 Router
JH296A	HP MSR954 1GbE+SFP Router
JH297A	HP MSR954-W 1GbE+SFP (WW) Router
JH298A	HP MSR954-W 1GbE+SFP LTE (AM) Rtr

JH299A	HP MSR954-W 1GbE+SFP LTE (WW) Rtr
JM044A	HPE MSR3620 Router
JM045A	RT-MPU-100-X1
JM046A	RT-SPU-400-X1
R8V33A	HPE MSR1002X 4 AC Router
R8V32A	HPE MSR3016 AC Router
R9J03A	HPE MSR3026 Router
R9J04A	HPE MSR3046 Router
R9J05A	HPE MSR3048 Router
S0W31A	HPE MSR954-V2 1GbE SFP Router

Table 3 MSR1000/MSR2000/MSR3000/MSR4000 Hardware and software compatibility matrix

Item	Specifications			
Product family	MSR1000_MSR2000_MSR3000_MSR4000 MSR958 MSR954-D4G MSR954_MSR954-V2 MSR 3620-DP MSR 56-60_MSR 56-80 MSR1002X4 MSR30X6 MSR30X8			
Boot ROM version	MSR1002-4_MSR1003-8S: 273 or higher MSR2003_MSR2004-24_MSR2004-48: 183 or higher MSR3012_MSR3024_MSR3044_MSR3064: 182 or higher MSR4060_MSR4080: MPU-100: 171 or higher SPU-100/200: 150 or higher MPU-100-X1: 242 or higher SPU-400-X1: 220 or higher MSR958: 132 or higher MSR954-D4G: 120 or higher MSR954_MSR954-V2: 167 or higher MSR1002X4: 100 or higher MSR3016: 132 or higher MSR3026_MSR3046_MSR3048: 103 or higher			
Host software	Hardware	software	MD5 Check Sum	File size
	MSR2003_MSR2004-24_MSR2004-48	MSR2000-CMW7 10-R6749P14.ipe	24a11c507a48cf9c070bce79f43d08e5	103,635,968 bytes
	MSR3012_MSR3024_MSR3044_MSR3064_MSR3620-DP	MSR3000-CMW7 10-R6749P14.ipe	393f206f5c7221e43658e496b86f8bb7	124,698,624 bytes

	MSR4060_MSR4080_MSR56-60_MSR56-80	MSR4000-CMW710-R6749P14.ipe	a242818aa63477d0a8b0db0c39fd7c4d	200,401,920 bytes
	MSR1002-4_MSR1003-8S	MSR100X-CMW710-R6749P14.ipe	0d5a988e711c03db7ee9990b0989cc01	105,029,632 bytes
	MSR954	MSR954-CMW710-R6749P14.ipe	5d3cfa28e713947d286a24eafad01e2e	111,887,360 bytes
	MSR954-D4G	MSR954P-CMW710-R6749P14.ipe	094207e9572ace4c4caec5ffd08ad608	71,321,600 bytes
	MSR958	MSR958-CMW710-R6749P14.ipe	945868691305d837fe31af64e3e2d292	109,644,800 bytes
	MSR1002X4	MSR1000X-CMW710-R6749P14.ipe	20019c3845207af1f3767f70e37806d8	111,122,432 bytes
	MSR3016_MSR3026_MSR3046	MSR30X6-CMW710-R6749P14.ipe	0ec7ffe4a0c5560e05514c7aa8d2d91e	128,039,936 bytes
	MSR3048	MSR30X8-CMW710-R6749P14.ipe	96b6414f2f14330f0319b72f190eded8	126,970,880 bytes
iMC version	iMC FCAPS(E0709) iMC AOM(E0706P01) iMC ACLM (E0706P12) iMC BIMS 7.3 (E0509) iMC DM 7.3(E0706P12) iMC EAD 7.3 (E0627) iMC EIA 7.3 (E0627) iMC EIA 7.3 (E0627) iMC ICC 7.3(E0706P12) iMC IVM 7.3 (E0508) iMC MVM 7.3 (E0511) iMC NTA 7.3 (E0507) iMC PLAT 7.3 (E0706P12) iMC QoSM 7.3 (E0506P01) iMC SHM 7.3 (E0511) UCenter E0709 iMC VLAN 7.3 (E0706P12)			
iNode version	iNode PC 7.3 (E0585)			
Cards version	Cards Name	Software Version	CPLD or FPGA version	
	SIC-3G-HSPA	280 or higher	200 or higher	
	SIC-3G-CDMA	280 or higher	200 or higher	

Upgrade advice

As a best practice, upgrade to this version as long as possible.

Upgrading restrictions and guidelines

1. After the software is upgraded from a version earlier than E0302P06 to E0302P06 or a later version, the unit of the VRRP preemption delay is changed from seconds to centiseconds.
2. Congestion might occur on the SIC-4SAE/2SAE interface modules with the FPGA version as 2.0. To solve this problem, manually upgrade the FPGA from version 2.0 to version 3.0.

Hardware feature updates

For hardware feature changes in version R0707P24 and earlier for MSR954_MSR954P_MSR958 series routers, see *HPE MSR954_MSR954P_MSR958-CMW710-R0707P24 Release Notes*

CMW710-R6749P14

Add new hardware:

SOW32A (HPE MSR 4p Gig-T HMIM-V2 Mod)

SOW33A (HPE MSR 8p Gig-T HMIM-V2 Mod)

SOW34A (HPE MSR 8p 1000BASE-X HMIM-V2 Mod)

SOW35A (HPE MSR 16p Enh Async Serial HMIM-V2 Mod)

SOW31A (HPE MSR954-V2 1GbE SFP Router)

CMW710-R6728P25

None.

CMW710-R6728P20

None.

CMW710-R6728P15

Add new hardware:

RT-SIC-4GSWF

CMW710-R0821P11

None.

CMW710-R0809P33

None.

CMW710-R0809P32

None.

CMW710-R0809P29

None.

CMW710-R0809P27

None.

CMW710-R0707P24

None

CMW710-R0707P21

None

CMW710-R0707P19

None

CMW710-R0707P16

None

CMW710-R0707P12

None

Software feature and command updates

For software feature changes in version R0707P24 and earlier for MSR954_MSR954P_MSR958 series routers, see *HPE MSR954_MSR954P_MSR958-CMW710-R0707P24 Release Notes* (Software Feature Changes).

For more information about the software feature and command update history, see *HPE MSR1000_MSR2000_MSR3000_MSR4000_MSR9XX-CMW710-R6749P14 Release Notes* (Software Feature Changes).

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
CMW710-R6749P14			
New	None	None	None
Modified	None	None	None
CMW710-R6728P20			
New	None	None	None
Modified	None	None	None
CMW710-R6728P15			
New	None	None	None
Modified	None	None	None
CMW710-R0821P11			
New	None	None	None
Modified	None	None	None
CMW710-R0809P33			
New	None	None	None
Modified	None	None	None
CMW710-R0809P32			
New	None	None	None
Modified	None	None	None
CMW710-R0809P29			
New	None	None	None
Modified	None	None	None
CMW710-R0809P27			
New	None	None	None
Modified	None	None	None
CMW710-R0707P24			
New	None	None	None
Modified	None	None	None
CMW710-R0707P21			
New	None	None	None
Modified	None	None	None
CMW710-R0707P19			
New	None	None	None
Modified	None	None	None

CMW710-R0707P16			
New	None	None	None
Modified	None	None	None
CMW710-R0707P12			
New	None	None	None
Modified	None	None	None

Operation changes

None

Restrictions and cautions

Restrictions

1. HPE's FXS not supporting call transfers from an analog phone to Lync Server.
2. The mGRE and Suite B features are not available in the current software version R04XX.
3. To upgrade from R0305 to R0305P04 or a later version, you must first install the R0305H01 hot patch.
4. MSR1000_2000_3000_4000_1000X_30X6_30X8 series and MSR954_MSR954P_MSR958 series do not support CFD.
5. The traffic statistics for a Layer 3 aggregate subinterface do not contain error packet statistics. Comparatively, the traffic statistics for a Layer 3 aggregate interface contain error packet statistics. To diagnose error packets received and sent on a Layer 3 aggregate subinterface, use the traffic statistics of member physical links and the aggregate interface for analysis and inference.

Open problems and workarounds

202301300158

- Symptom: A 10G port on an MSR3016、MSR3026、MSR3046 router comes up and goes down repeatedly.
- Condition: This symptom occurs if two optical fibers are used to connect a 10G fiber port on an MSR36X1 router to the peer and you remove one of the two optical fibers after the port comes up.
- Workaround: When one of the two optical fibers that connect a port is faulty, replace the faulty optical fiber in time. Alternatively, you can remove also the other optical fiber and then insert two normal optical fibers together.

202306071242

- Symptom: An EAA track event monitor policy fails to be deployed.
- Condition: This symptom occurs if you configure an EAA track event monitor policy by using Tcl.
- Workaround: Configure an EAA track event monitor policy from the CLI.

202306090461

- Symptom: The UDP port is not disabled after an SNMP notification target host is removed and the information center is disabled.

- Condition: This symptom occurs after an SNMP notification target host is removed and the information center is disabled.
- Workaround: None. This issue does not affect the functionality of the device and is scheduled to be fixed in the next version.

202306130779

- Symptom: 128 traps are generated.
- Condition: This symptom occurs if VA interfaces are created or deleted on an L2TP network
- Workaround: None. This issue does not affect the functionality of the device and is scheduled to be fixed in the next version.

202306190522

- Symptom: The forwarding performance is low on an interface.
- Condition: This symptom might occur if you assign a Layer 2 interface on an MSR3048 to a VLAN and configure the VLAN interface to forward traffic.
- Workaround: Use Layer 3 interfaces or Layer 3 subinterfaces.

List of resolved problems

For resolved problem lists of version R0707P24 and earlier for MSR954_MSR954P_MSR958 series routers, see *HPE MSR954_MSR954P_MSR958-CMW710-R0707P24 Release Notes*

Resolved problems in CMW710-R6749P14

None.

Resolved problems in CMW710-R6728P25

202206240760

- Symptom: The shell command is lost for the corresponding tty after the operating mode of an asynchronous serial interface is changed to protocol and then changed back to flow.
- Condition: This symptom occurs after the operating mode of an asynchronous serial interface is changed to protocol and then changed back to flow.

202205121202

- Symptom: Formatting files by using an SSH terminal fails when there is only one SSH terminal using the file system.
- Condition: This symptom occurs if you use an SSH terminal to format files.

202206281099

- Symptom: RBAC registration alarms are printed when an IRF fabric starts up.
- Condition: This symptom occurs when an IRF fabric starts up.

202206090402

- Symptom: On the Web interface, an internal error message is displayed when a service provider address base file is imported.
- Condition: This symptom occurs when you import a service provider address base file that has a Chinese file name on the Modify Multi-WAN Policy tab.

202112230150

- Symptom: After an interface on an MSR router is changed to Layer 3 mode, the Maximum frame length field is not displayed in the display interface command output.
- Condition: This symptom occurs after an interface on an MSR router is changed to Layer 3 mode.

202201260604

- Symptom: An MSR4000 router drops a small number of incoming packets on an interface of an SPU-400-x1 card when the total traffic rate exceeds 10% of the interface bandwidth.
- Condition: This symptom occurs if the interface receives both IPv4 packets and IPv6 packets.

202208191102

- Symptom: The virtual IP address of the VRRP group is not reachable if the aggregate interface on the MSR3026 has multiple member ports.
- Condition: This symptom occurs if the Layer 3 aggregate interface has multiple member ports, and is enabled with VRRP.

202210110714

- Symptom: Removal of a SIC-5G subcard is not reported to the controller. Normal event will not be reported to the controller for subcard removal.
- Condition: This symptom occurs if the device is incorporated by the controller and a SIC-5G subcard is hot swapped.

202211100976

- Symptom: An MSR 4080 router fails to forward NAT traffic because the primary traffic processing slot of a subinterface is incorrect.
- Condition: This symptom occurs if both IRF and outbound NAT are configured.

202209291164

- Symptom: When IPCP NAK packets with the IPv4 option as all-zeros are received, the pppd process gets stuck in an infinite loop.
- Condition: This symptom occurs if the device receives invalid IPCP NAK packets (with the IPv4 option as all-zeros).

202210241602

- Symptom: The packets processed by RIR on the VSI inbound interface are encrypted and then processed in one core, the aging is slow in the RIR forwarding cache. When a large amount of traffic exists for a long period of time, the memory usage is high.
- Condition: This symptom occurs if packets processed by RIR on the VSI inbound interface.

202211140193

- Symptom: After a branch site is added to the network of the ADWAN solution, RIR link selection from the headquarters to the site is incorrect. Link selection is as expected after you configure the **tunnel out-interface** command again.
- Condition: This symptom occurs if you add a new site to the network of the ADWAN solution configured with RIR link selection.

Resolved problems in CMW710-R6728P20

202206150848

- Symptom: A line card reboots unexpectedly.

- Condition: This symptom might occur if a third-party 40km transceiver module is installed.

202205311764

- Symptom: The CVE-1999-0524 vulnerability exists.
- Condition: This symptom occurs when you scan the system for vulnerabilities.

202205190739

- Symptom: Establishment of RIR NQA detection fails.
- Condition: This symptom might occur if IRF member devices reboot and the traffic outgoing interface for a tunnel is on the subordinate device.

202205201580

- Symptom: An IRF master reboots unexpectedly.
- Condition: This symptom might occur if the device is in an ADWAN environment and traffic is scheduled by RIR after the device is powered on.

202204270732

- Symptom: IRF member devices reboot unexpectedly.
- Condition: This symptom might occur if last hop holding is enabled on the devices and FTP traffic is forwarded across the IRF master and subordinate devices.

202205181795

- Symptom: BGP connections are disrupted because of memory exhaustion.
- Condition: This symptom might occur if BGP routes are recurve to FRR routes and BGP route flapping occurs frequently.

202205121082

- Symptom: The GE0/0 and GE0/5 interfaces operate in Layer 2 mode by default on the device.
- Condition: This symptom might occur if the device boots with initial configuration or the default command has been executed on the interfaces.

Resolved problems in CMW710-R6728P15

202103310929

- Symptom: Memory leaks occur after IPv6 NetStream is configured.
- Condition: This symptom might occur if the device receives traffic after IPv6 NetStream is configured.

Resolved problems in CMW710-R0821P11

202102220319

- Symptom: The MSR3012 router might reboot unexpectedly when an EVI tunnel is forwarding traffic in both directions.
- Condition: This symptom occurs when an EVI tunnel is forwarding traffic in both directions.

Resolved problems in CMW710-R0809P33

202012081289

- Symptom: The device reboots after running for a long time because of memory exhaustion.
- Condition: This symptom occurs if the SNMP module is configured to send trap messages to multiple servers with the address of the first server reachable but the address of the second server unreachable.

202009300258

- Symptom: The IKE process is stuck and tunnel negotiations fail.
- Condition: This symptom might occur in the following situation:
 - IKE uses digital certificate authentication, and the certificate revocation checking method is configured as **revocation-check method crl none**.
 - There are many IKE negotiations and the device cannot connect to the CRL repository server.

Resolved problems in CMW710-R0809P32

202009300258

- Symptom: The IKE process is stuck and tunnel negotiation fails.
- Condition: This symptom might occur if the following conditions exist:
 - IKE uses digital certificate authentication, and the certificate revocation checking method is configured as revocation-check method crl none.
 - There are many IKE negotiations and the device cannot connect to the CRL repository server.

202010100134

- Symptom: Deadloops and unexpected forwarding module reboots might occur after session statistics collection is enabled.
- Condition: This symptom might occur if DPI and session statistics collection are enabled and a large number of applications have application layer traffic.

Resolved problems in CMW710-R0809P29

202006220254

- Symptom: The free IP configuration does not take effect on an interface.
- Condition: This symptom occurs if 802.1X is disabled on another interface.

202006280603

- Symptom: The certificate server supports certificate renewal. During certificate renewal, the device does not sign the certificate request message sent to the server by using the current certificate.
- Condition: This symptom occurs when the device renews a certificate.

202005140088

- Symptom: The device might use an expired RA certificate for certificate request or renewal.

- Condition: This symptom might occur when the device has an expired RA certificate.

Resolved problems in CMW710-R0809P27

202003041116

- Symptom: A QoS policy containing a traffic policing action does not take effect on an aggregate interface.
- Condition: This symptom occurs if there is traffic on the aggregate subinterfaces instead of the aggregate interface and you apply the QoS policy to the aggregate interface.

202003190408

- Symptom: Cannot create an IPsec policy in the Web interface. An error message prompts that the configuration object does not exist.
- Condition: This symptom occurs after the device is restored to factory defaults.

202003130974

- Symptom: The renegotiation initiated by the local device failed.
- Condition: This symptom occurs when an IPsec tunnel is established between two IPsec gateways and you modify different IPsec policy entries of the same IPsec policy.

202003191478

- Symptom: The IKE process exited exceptionally, and memory overlap occurs.
- Condition: This symptom occurs if you execute the **reset advpn session** command or the **reset vam client fsm** command when CRL checking is enabled.

202006100361

- Symptom: An interface might fail to receive or send packets with a low probability, which will cause traffic forwarding failure.
- Condition: This symptom occurs if a device with an HMIM-4GEE or HMIM-4GEF card is upgraded to version R0809 and the peer device is not restarted.

202005190442

- Symptom: The username checking feature cannot be disabled by the undo password-control complexity user-name check command.
- Condition: This symptom occurs if you execute the undo password-control complexity user-name check command in local user view or user group view.

201912131149

- Symptom: Ping failure or service exception exists for ping or service packets (for example, Telnet or DDNS) sourced from the local device.
- Condition: This symptom might occur if dual WAN links are available for the packets.

202005061081

- Symptom: The IKE process cannot be started because of failure to bind default port 500 to IKE.
- Condition: This symptom occurs if you configure IKE when port 500 is occupied by using the **nqa server udp-echo x.x.x.x 500** command.

202006180450

- Symptom: A memory exception is detected during the MPU booting process.
- Condition: This symptom might occur if a tool is used to check the memory for exceptions during the MPU booting process.

202007030293

- Symptom: The device mistakenly dropped ARP broadcast packets when the time counter of ARP is reversed.
- Condition: This symptom occurs if the time counter of ARP is reversed.

Resolved problems in CMW710-R0707P24

201911060979

- Symptom: The source IP address or destination network segment address configuration is displayed as a host address in the Web interface.
- Condition: This symptom occurs if the following operations are performed on the authentication-free IP address page in the Web interface:
 - a. Configure a description.
 - b. Set the source IP address or destination network segment address.

201910310870

- Symptom: The server IP address cannot be modified.
- Condition: This symptom might occur if you select both the check box for modifying server address and the check box for modifying the service provider on the advanced options page.

201910250289

- Symptom: Configuration import operation might fail.
- Condition: This symptom might occur if the device has multiple storage media and you use the Web interface to import the configuration file.

201910241082

- Symptom: The Delete button to the right of a user group member does not take effect.
- Condition: This symptom might occur when you add or edit a user group on the Network Behaviors > User Group Configuration page.

201910240455

- Symptom: The IP address information is not displayed on the interface speed page or WAN configuration page.
- Condition: This symptom occurs if a Layer 3 WAN interface is configured to obtain an IP address through DHCP or PPPoE in the Web interface.

201910230726

- Symptom: The network behavior management feature is disabled.
- Condition: This symptom might occur if you specify the same string in different cases as the names for policies on the Web application control page.

201910230699

- Symptom: Cannot create a policy on the URL filtering page.
- Condition: This symptom might occur if you specify a policy name that starts with an upper-case letter.

201910150870

- Symptom: The later added IKE keychain will overwrite the previously added IKE keychain. As a result, only one IKE keychain exists on the device, and the IPsec tunnel might fail to be established.

- Condition: This symptom occurs if IPsec policies with the same letters of different cases in their names are added in order.

201910141007

- Symptom: The system fails to read the user information during user information modification.
- Condition: This symptom might occur when you modify a user on the Web user management page.

201910211052

- Symptom: Some configurations for AP templates of models WA2620-WiNet and WA2620E-WiNet get lost after you upgrade the AC from R0615PXX to R0707P21 because templates of the two models do not support the vlan1 command.
- Condition: This symptom might occur if you upgrade the AC from R0615PXX to R0707P21 and the vlan1 command has been executed for AP templates of the two models.

202002130717

- Symptom: A device reboots unexpectedly.
- Condition: This symptom occurs with a low probability if a multi-core device forwards multiple flows in a VXLAN/EVI environment.

201912020343

- Symptom: Before a user passes 802.1X authentication, the user cannot ping the configured EAD free IP.
- Condition: This symptom occurs if you configure the EAD free IP function and then enable 802.1X authentication.

201912190196

- Symptom: The SSH connection to the device is disconnected and core files are generated.
- Condition: This symptom occurs if the password control function is enabled, an SSH user logs in to the device for the first time, and the user enters incorrect passwords multiple times.

201912260565

- Symptom: LSAs remain in an OSPF NSSA area because of time sequence problems.
- Condition: This symptom occurs with a low probability if the device and its neighbor repeatedly enable and disable redistribution for the same routes.

201911291010

- Symptom: The memory of the device is lost.
- Condition: This symptom occurs if DPI is enabled on the device, two PCs share and access files across slots or chassis, and the device forwards SMB2 packets.

Resolved problems in CMW710-R0707P21

201911060528

- Symptom: The switch reboots because of memory exhaustion.
- Condition: This symptom occurs if the switch forwards traffic for a long time when application statistics collection or session statistics collection is enabled.

201908300153

- Symptom: A server returned an HTTPS authentication failure report during TACACS authentication.

- Condition: This symptom might occur when the rem_addr field of the authentication request does not carry the terminal IP address but a server identifies the processing policy based on the field.

201907190401

- Symptom: CFD does not take effect.
- Condition: This symptom occurs if CFD is configured on the device and then the device is rebooted.

201907300197

- Symptom: An error is reported during the operating system installation on VMs.
- Condition: This symptom occurs if the operating system is installed in the same disk on two VMs.

201909240203

- Symptom: The IP addresses are not displayed on the IP address list page.
- Condition: This symptom occurs if multiple WAN interfaces obtain IP addresses through DHCP and PPPoE links.

Resolved problems in CMW710-R0707P19

201906120398

- Symptom: ADVPNs fail to be established.
- Condition: This symptom occurs if multiple spokes use different addresses and ports to register ADVPN negotiation.

201906240172

- Symptom: The memory leaks.
- Condition: This symptom occurs if the info-center syslog trap buffersize 65535 command is executed and the device runs for a long period of time.

201907040419

- Symptom: Traffic from some addresses might be switched to the backup link when the primary link works correctly.
- Condition: This symptom might occur in an MPLS L3VPN FRR scenario.

201908120849

- Symptom: The Web interface hangs. No operations can be performed.
- Condition: This symptom occurs after you click the close button (a cross) in the top right corner of the **Protected Configuration** page (IPsec protected data flow configuration page).

Resolved problems in CMW710-R0707P16

201905230062

- Symptom: The TACACS server cannot recover from the Block status.
- Condition: This symptom occurs if active/standby switchover occurs on the device.

201905220166

- Symptom: Static route configuration is lost.
- Condition: This symptom occurs if the route configuration contains interfaces and descriptions, and the IRF mode is switched.

201905230358

- Symptom: Errors occur to LLDP initialization.
- Condition: This symptom occurs if the subordinate member device of an IRF fabric is rebooted.

201905230130

- Symptom: The link aggregation module operates abnormally.
- Condition: This symptom occurs if links flap.

201905230155

- Symptom: Telnet users remain.
- Condition: This symptom occurs if users repeatedly Telnet to the device through different terminals.

201905200886

- Symptom: The device cannot properly forward packets.
- Condition: This symptom occurs if the device is configured with the **vpn popgo** command.

Resolved problems in CMW710-R0707P12

201802270338

- Symptom: QoS does not take effect.
- Condition: This symptom occurs if QoS is enabled on the VT interface bound to an E1 interface and the VT interface is shut down and then brought up.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
www.hpe.com/support/hpesc

Information to collect:

- Technical support registration number (if applicable).
- Product name, model or version, and serial number.
- Operating system name and version.
- Firmware version.
- Error messages.
- Product-specific reports and logs.
- Add-on products or components.
- Third-party products or components.

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website at <http://www.hpe.com/support/hpesc>.

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see HPE FlexNetwork technology acronyms.

Related documents

The following documents provide related information:

- HPE FlexNetwork MSR2000 Routers Installation Guide
- HPE FlexNetwork MSR3000 Routers Installation Guide
- HPE FlexNetwork MSR4000 Routers Installation Guide
- HPE FlexNetwork MSR2000 Routers Quick Start
- HPE FlexNetwork MSR3000 Routers Quick Start
- HPE FlexNetwork MSR4000 Routers Quick Start
- HPE FlexNetwork MSR Router Series Interface Module Guide
- HPE FlexNetwork MSR2000/3000/4000 Routers Compliance and Safety Manual
- HPE FlexNetwork MSR954 Routers Quick Start
- HPE FlexNetwork MSR954 Routers Installation Guide
- HPE FlexNetwork MSR958 Routers Quick Start
- HPE FlexNetwork MSR958 Routers Installation Guide
- About the HPE FlexNetwork MSR Router Series Command References(V7)
- HPE FlexNetwork MSR Router Series ACL and QoS Command Reference(V7)
- HPE FlexNetwork MSR Router Series EVI Command Reference(V7)
- HPE FlexNetwork MSR Router Series Fundamentals Command Reference(V7)
- HPE FlexNetwork MSR Router Series High Availability Command Reference(V7)
- HPE FlexNetwork MSR Router Series Interface Command Reference(V7)
- HPE FlexNetwork MSR Router Series IP Multicast Command Reference(V7)
- HPE FlexNetwork MSR Router Series Layer 2 - LAN Switching Command Reference(V7)
- HPE FlexNetwork MSR Router Series Layer 2 - WAN Access Command Reference(V7)
- HPE FlexNetwork MSR Router Series Layer 3 - IP Routing Command Reference(V7)
- HPE FlexNetwork MSR Router Series Layer 3 - IP Services Command Reference(V7)
- HPE FlexNetwork MSR Router Series MPLS Command Reference(V7)
- HPE FlexNetwork MSR Router Series NEMO Command Reference(V7)
- HPE FlexNetwork MSR Router Series Network Management and Monitoring Command Reference(V7)
- HPE FlexNetwork MSR Router Series OAA Command Reference(V7)
- HPE FlexNetwork MSR Router Series OpenFlow Command Reference(V7)
- HPE FlexNetwork MSR Router Series Probe Command Reference(V7)
- HPE FlexNetwork MSR Router Series Security Command Reference(V7)

- HPE FlexNetwork MSR Router Series Virtual Technologies Command Reference(V7)
- HPE FlexNetwork MSR Router Series Voice Command Reference(V7)
- HPE FlexNetwork MSR Router Series WLAN Command Reference(V7)
- About the HPE FlexNetwork MSR Router Series Configuration Guides(V7)
- HPE FlexNetwork MSR Router Series ACL and QoS Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series EVI Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Fundamentals Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series High Availability Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Interface Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series IP Multicast Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Layer 2 - LAN Switching Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Layer 2 - WAN Access Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Layer 3 - IP Routing Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Layer 3 - IP Services Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series MPLS Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series NEMO Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Network Management and Monitoring Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series OAA Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series OpenFlow Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Probe Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Security Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Virtual Technologies Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series Voice Configuration Guide(V7)
- HPE FlexNetwork MSR Router Series WLAN Configuration Guide(V7)

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Appendix A Feature list

Hardware features

Table 5 MSR1000 specifications

Item	MSR1002-4	MSR1003-8S
Console/AUX port	1	1
USB port	1	1
Gigabit Ethernet port	5	10
SFP port	1	N/A
Asynchronous/synchronous serial interface	1	N/A
Memory	1 GB DDR3	1 GB DDR3
Flash	256 MB	256 MB
SIC/DSIC slot	2 SIC slot (1 DSIC slot)	3 SIC slots (1 DSIC slot)
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	44.2 × 360 × 300 mm (1.74 × 14.17 × 11.81 in)	44.2 × 360 × 300 mm (1.74 × 14.17 × 11.81 in)
AC power supply	Rated voltage range: 90 VAC to 264 VAC @ 50 Hz/60 Hz	Rated voltage range: 90 VAC to 264 VAC @ 50 Hz/60 Hz
Rated power for AC power supply	30 W	30 W
Operating temperature	0°C to 45°C (32°F to 113°F)	0°C to 45°C (32°F to 113°F)
Relative humidity (noncondensing)	5% to 90%	5% to 90%

Table 6 MSR2000/MSR2000 TAA specifications

Item	MSR2003/MSR2003T AA	MSR2004-24	MSR2004-48
Console/AUX port	1	1	1
USB console port	1	-	-
USB port	1	1	1
GE WAN port	2		
GE LAN port	-	3	3
SFP port	-	1	-
Memory	1GB DDR3	1GB DDR3	1GB DDR3
Flash/CF	256MB Flash	256MB CF	256MB CF
SIC/DSIC slot	3 SIC slots (Slots 1 and 2 can be used for a DSIC interface module by removing the slot divider.)	4 SIC slots	4 SIC slots

Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	360mm×305.3mm×44.2 mm	440mm×363.5mm×44.2	440mm×403.5mm×44.2
AC power supply	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz/60 Hz		
DC power supply	-	-	Rated voltage range: -48V d.c. ~ -60V d.c
Maximum power for AC/DC power supply	54W	54W	150W
Operating temperature	0 ~ 45°C		
Relative humidity (noncondensing)	5% to 90%		

Table 7 MSR3000/MSR3000 TAA specifications

Item	MSR3012	MSR3024/MSR 3024 TAA	MSR3044	MSR3064
CON/AUX ports	1			
USB console ports	1			
USB ports	2			
Gigabit Ethernet ports	3			
SIC/DSIC slots	2 SIC slots		4 SIC slots/2 DSIC slots	
HMIM slots	1	2	4	6
VPM slots	1	1	2	2
Memory	DDR3 1 GB/2 GB	DDR3 2 GB (default) 4 GB (maximum)	DDR3 2 GB (default) 4 GB (maximum)	
CF card memory (inside)	256 MB (default)			
CF card memory (outside)	-		4 GB (maximum)	
CF card slot	0		1	
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	44.2 × 440 × 484.3 mm	44.2 × 440 × 484.3 mm	88.1 × 440 × 480 mm	130.5 × 440 × 480 mm
AC power supply	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz/60 Hz			
DC power supply	Rated voltage range: −48 VDC to −60 VDC			
Maximum power for AC/DC power supply	125 W	125 W	300 W	300 W
Maximum power for PoE power supply	-	275 W	750 W	750 W
Maximum power for each PoE port	15.4 W			

RPS power supply	800 W	-
Power pluggable and backup	-	Dule power
Operating temperature	0°C to 45°C (32°F to 113°F)	
Relative humidity (noncondensing)	5% to 90%	

Table 8 MSR4000 specifications

Item	MSR4060	MSR4080
MPU slot	2	
SPU slot	1	
HMIM slot	6	8
Dimensions (H × W × D), excluding rubber feet and mounting brackets	175.1 × 440 × 480 mm	219.5 × 440 × 480 mm
Power pluggable and backup	N+1	N+1
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity (noncondensing)	5% to 90%	

Table 9 MSR4000/MSR4000 TAA MPU Specification

Item	Specification
Console port	1
AUX port	1
GE management port	1
USB console port	1
USB port	1
Memory	2 GB DDR3 (default) 4 GB DDR3 (maximum)
CF card	512 MB (default) 4 GB (maximum)
CF card slot	1
Flash	8 MB

Table 10 MSR4000 SPU Specification

Item	SPU-100	SPU-200&SPU-300
USB port	2	
VPM slot	2	

Combo	4	
SFP+ port	0	1
Applicable router model	MSR4060/MSR4080	
Applicable MPU	MPU-100	

Table 11 MSR2004-24 AC power module specifications

Item	Specification
Rated input voltage range	100 VAC to 240 VAC @ 50 Hz or 60 Hz
Rated power	150 W

Table 12 MSR2004-48 DC power module specifications

Item	Specification
Rated input voltage range	–48 VDC to –60 VDC
Rated power	150 W

Table 13 MSR3044/MSR3064/MSR4060/MSR4080 AC power module specifications

Item	Specification
Model	PSR300-12A1
Rated input voltage range	100 VAC to 240 VAC @ 50 Hz or 60 Hz
Max power	300 W

Table 14 MSR3044/MSR3064/MSR4060/MSR4080 DC power module specifications

Item	Specification
Model	PSR300-12D2
Rated input voltage range	–48 VDC to –60 VDC
Max power	300 W

Table 15 MSR3044/MSR3064/MSR4060/MSR4080 PoE power module specifications

Item	Specification
Model	PSR750-A
Rated input voltage range	100 VAC to 240 VAC @ 50 Hz or 60 Hz
Max power	750 W

Table 16 MSR954P_MSR958 specifications

Item	JH300A	JH301A	JH373A
Console port	1		

Item	JH300A	JH301A	JH373A
USB port	1		
GE WAN port	1GE+1Combo	1GE+1Combo	1GE
GE LAN port	8	8	4
Memory	DDR III 1GB		
Flash	256MB		
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	330×230×44.2mm	330×230×44.2mm	300×200×44.2mm
AC power adapter	100V AC~240V AC, 50Hz~60Hz		
Max. AC power	20W	20W+65W(PoE)	24W
Operating temperature	0℃~45℃	0℃~45℃	0℃~40℃
Relative humidity (non-condensing)	5%~90%		

Table 17 MSR954 specifications

Item	JH296A	JH297A	JH298A	JH299A
Console port	1			
USB port	2	2	1	1
GE WAN port	2			
GE LAN port	4			
Memory	DDR III 1GB			
Flash	256MB			
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	43.6 × 266 × 161 mm (1.72 × 10.47 × 6.34 in)			
AC power adapter	100V AC~240V AC, 50Hz~60Hz			
Max. AC power	15W			
Operating temperature	0℃~45℃			
Relative humidity (non-condensing)	5%~90%			

Table 18 MSR1002X 4 technical specifications

Item	MSR1002X 4
Console/AUX port	N/A
Console port	1
USB port	1
Gigabit Ethernet port	5
SFP port	1

Item	MSR1002X 4
Asynchronous/synchronous serial interface	1
Memory	1GB DDR3
Flash	512 MB
SIC/DSIC slot	2 SIC slots
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	44.2 × 360 × 300 mm (1.74 × 14.17 × 11.81 in)
AC power supply	Rated voltage range: 90 VAC to 264 VAC @ 50 Hz/60 Hz
Rated power for AC power supply	36 W
Operating temperature	0°C to 45°C (32°F to 113°F)
Relative humidity (noncondensing)	5% to 95%

Table 19 MSR30X6/MSR30X8 TAA specifications

Item	MSR3016	MSR3026	MSR3046	MSR3048
Console ports	1	1	1	1
USB ports	1	1	1	1
Gigabit Ethernet WAN ports	4 (two combo ports)	8	9 (one is a combo port)	10
Gigabit Ethernet LAN/WAN ports	N/A	8	N/A	N/A
SFP ports	4 (two combo ports)	N/A	1 (combo port)	N/A
SFP+ ports	N/A	6	5	16
SFP28 ports	N/A	N/A	N/A	4
SIC/DSIC slots	4 SIC slots	4 SIC slots	4 SIC slots	4 SIC slots
HMIM slots	N/A	2	4	4
Hard disk	1 (2.5 inch, SATA connectors)	N/A	N/A	N/A
Memory	2 GB DDR4	4 GB DDR4	4 GB DDR4	8 GB DDR4
Flash memory	512 MB	1 GB	1 GB	1 GB
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	43.6 × 440 × 360 mm (1.72 × 17.32 × 14.17 in)	44.2 × 440 × 470 mm (1.74 × 17.32 × 18.50 in)	88.1 × 440 × 480 mm (3.47 × 17.32 × 18.90 in)	88.1 × 440 × 480 mm (3.47 × 17.32 × 18.90 in)
Power supply slots	N/A	2	2	2

Item	MSR3016	MSR3026	MSR3046	MSR3048
AC power input	Single AC input	N/A	N/A	N/A
AC power supply	Rated voltage range: 100 VAC to 240 VAC @ 50 Hz/60 Hz			
DC power supply	N/A	Rated voltage range: -48 VDC to -60 VDC	Rated voltage range: -48 VDC to -60 VDC	Rated voltage range: -48 VDC to -60 VDC
Max power of the power supplies	N/A	150 W	300 W	300 W
Operating temperature	- With a hard disk: 5°C to 40°C (41°F to 104°F) - Without a hard disk: 0°C to 45°C (32°F to 113°F)	0°C to 45°C (32°F to 113°F)	0°C to 45°C (32°F to 113°F)	0°C to 45°C (32°F to 113°F)
Humidity	5% RH to 95% RH (noncondensing)			

Table 20 MSR954-V2 specifications

Item	S0W31A
Console port	1
USB port	1
GE WAN port	1
GE SFP port	1
GE LAN port	4
Serial port	N/A
Memory	1 GB DDR3
Flash	256 MB
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	44 × 210 × 140 mm (1.73 × 8.27 × 5.51 in)
AC input voltage	100 VAC to 240 VAC @ 50 Hz/60 Hz
Max. AC power	24 W
Operating temperature	0°C to 40°C (32°F to 104°F)
Relative humidity (non-condensing)	5% to 90%

Table 21 MSR series routes Module List

Module	Description
SIC	Ethernet interface modules: 4-port 10/100 Mbps Ethernet L2 switching module (RJ45) (SIC-4FSW) 1-port 10/100 Mbps Ethernet electrical SIC interface module (RJ45) (SIC-1FEA) 1-port 100 Mbps Ethernet electrical SIC interface module-SIC-1FEF 4-port 10/100 Mbps Ethernet L2 switching module-PoE card(SIC-4FSW-POE) 1-port 10/100/1000BASE-T(RJ45) and 100BASE-FX/1000BASE-X(SFP,Combo)Ethernet

	SIC module(RT-SIC-1GEC-V2(JG738A)) 4-port 10/100/1000BASE-T Ethernet L2 switching electrical SIC interface module(RT-SIC-4GSW(JG739A)) 4-port 10/100/1000BASE-T Ethernet L2 switching electrical SIC interface module-PoE(RT-SIC-4GSWP(JG740A)) - HPE FlexNetwork MSR 4-Port 1000BASE-X SIC Module-RT-SIC-4GSWF WAN interface modules: 1-port enhanced synchronous/asynchronous serial SIC interface module (SIC-1SAE) 1-port fractional E1 SIC interface module (SIC-1E1-F-V3) 1-port E1/CE1/PRI SIC interface module (SIC-1EPRI) 1-port analog modem SIC interface module (SIC-1AM) 8-port asynchronous serial interface card (SIC-8AS) 16-port asynchronous serial interface card (SIC-16AS) 1-port ISDN BRI S/T interface card (SIC-1BS) 2-port fractional E1 interface module (SIC-2E1-F) 3G access module (RT-SIC-3G-HSPA) - CDMA 2000 1x RTT/1x EV-DO Rev.0/1x EV-DO Rev.A 3G access module (RT-SIC-3G-CDMA) 1-port ADSL over POTS SIC interface module (SIC-1ADSL) 1 port E1/CE1/PRI SIC interface module(SIC-1EPRI-V3) 4G LTE Verizon SIC module(RT-SIC-4G-LTE-V(JG742A)) 4G LTE AT&T SIC module(SIC-4G-LTE-A(JG743A)) 4G LTE Global SIC module(RT-SIC-4G-LTE-G(JG744A)) 2-port enhanced synchronous/asynchronous serial SIC interface module(RT-SIC-2SAE(JG736A)) 4-port enhanced synchronous/asynchronous serial SIC interface module(RT-SIC-4SAE(JG737A)) - HPE MSR 4GLTE SIC Mod for CDMA/WCDMA (JG742B) - HPE MSR 4G LTE SIC Mod for ATT (JG743B) - HPE MSR 4GLTE SIC Mod for Global (JG744B) - HPE MSR HSPA+/WCDMA SIC Module (JG929A) Voice interface modules: 1-port voice module subscriber circuit SIC interface module (SIC-1FXS) 2-port voice module subscriber circuit SIC interface module (SIC-2FXS) 1-port voice module FXO SIC interface module (SIC-1FXO) 2-port voice module FXO SIC interface module (SIC-2FXO) 1-channel E1 voice SIC interface module (SIC-1VE1) 1-channel T1 voice SIC interface module (SIC-1VT1) 1-port ISDN BRI S/T voice interface card (SIC-1BSV) 2-port ISDN BRI S/T voice interface card (SIC-2BSV) 2-port voice subscriber circuit & 1-port voice AT0 analog trunk interface card-SIC-2FXS1FXO 1-port E1 / T1 Voice SIC Module(JH240A)
DSIC	9-port 10/100 Mbps Ethernet L2 switching module (RJ45) (DSIC-9FSW) 4-port voice subscriber circuit & 1-port voice AT0 analog trunk interface card (DSIC-4FXS1FXO) 9-port 10/100 Mbps Ethernet L2 switching module -PoE card (DSIC-9FSW-POE) 1-port 8-wire G.SHDSL (RJ45) DSIC Module
HMIM	Ethernet interface modules: 2-port 10M/100/1000M Ethernet electrical HMIM interface module (RJ45) (HMIM-2GEE)

- 4-port 10M/100/1000M Ethernet electrical HMIM interface module (RJ45) (HMIM-4GEE)
- 8-port 10M/100/1000M Ethernet electrical HMIM interface module (RJ45) (HMIM-8GEE)
- 2-port 1000BASE-X HMIM Module (HMIM-2GEF)
- 4-port 1000BASE-X HMIM Module (HMIM-4GEF)
- 8-port 1000BASE-X HMIM Module (HMIM-8GEF)
- 24-port Gig-T Switch HMIM Module (HMIM-24GSW)
- 24-port Gig-T PoE Switch HMIM Module (HMIM-24GSW-POE)
- 8-port 10/100/1000BASE-T(RJ45)+2-port 100BASE-FX/1000BASE-X(SFP,Combo) Ethernet L2 switching HMIM module(RT-HMIM-8GSW(JG741A))
- 8-port 100BASE-FX/1000BASE-X / 4-port 1000BASE-T (Combo) L2/L3 HMIM Module (JH238A)
- HPE FlexNetwork MSR 4-Port Gig-T L3 HMIM-V2 Module
- HPE FlexNetwork MSR 8-Port Gig-T L3 HMIM-V2 Module
- HPE FlexNetwork MSR 16-Port Enhanced Async Serial HMIM-V2 Module
- HPE FlexNetwork MSR 8-Port 1000BASE-X L3 HMIM-V2 Module

WAN interface modules:

- 2 port CE1/PRI interface module (HMIM-2E1)
- 4 port CE1/PRI interface module (HMIM-4E1)
- 8 port CE1/PRI interface module (HMIM-8E1)
- 4-port fractional E1 interface module (HMIM-4E1-F)
- 8-port fractional E1 interface module (HMIM-8E1-F)
- 2 port CT1/PRI interface module (HMIM-2T1)
- 8 port CT1/PRI interface module (HMIM-8T1)
- 4-port fractional T1 interface module HMIM-4T1-F)
- 8-port fractional T1 interface module HMIM-8T1-F)
- 1-port T3/CT3 compatible interface module (HMIM-1CT3)
- 1-port T3/CT3 compatible interface module (HMIM-1CE3)
- 2 channel enhanced synchronous/asynchronous interface module (HMIM-2SAE)
- 4 channel enhanced synchronous/asynchronous interface module (HMIM-4SAE)
- 8 channel enhanced synchronous/asynchronous interface module (HMIM-8SAE)
- 8 port asynchronous serial interface panel (RJ45) (HMIM-8ASE)
- 16 port asynchronous serial interface panel (RJ45) (HMIM-16ASE)
- 1-port OC-3 / STM-1 CPOS HMIM Module (HMM-1CPOS)
- 2-port OC-3 / STM-1 CPOS HMIM Module (HMIM-2CPOS)
- 1-port OC-3c / STM-1c ATM SFP HMIM Module (HMIM-ATMOC3)
- 8-port E1 / CE1 / T1 / CT1 / PRI HMIM Module (JH169A)
- 4-port E1 / CE1 / T1 / CT1 / PRI HMIM Module (JH170A)
- 2-port E1 / CE1 / T1 / CT1 / PRI HMIM Module (JH171A)
- 8-port E1 / Fractional E1 / T1 / Fractional T1 HMIM Module (JH172A)
- 4-port E1 / Fractional E1 / T1 / Fractional T1 HMIM Module (JH173A)
- 2-port E1 / Fractional E1 / T1 / Fractional T1 HMIM Module (JH174A)
- 1-port Clear Channel E3/T3 HMIM Module(JH449A)

Voice interface modules:

- 16-port voice module subscriber circuit interface board(HMIM-16FXS)
- 1 channel E1 voice HMIM interface module (HMIM-1VE1)
- 2 channel E1 voice HMIM interface module (HMIM-2VE1)
- 1 channel T1 voice HMIM interface module (HMIM-1VT1)
- 2 channel T1 voice HMIM interface module (HMIM-2VT1)

	4-port voice module subscriber circuit interface board (HMIM-4FXS) 4-port voice module FXO interface module (HMIM-4FXO) 4 channel voice processing board E&M trunk interface module (HMIM-4EM)
VPM	128-channel voice processing module (RT-VPM2-128) 256-channel voice processing module (RT-VPM2-256) 512-channel voice processing module (RT-VPM2-512)
HMIM Adapter	0.5U MIM to HMIM adapter (HMIM Adapter) 1U MIM to HMIM adapter (HMIM Adapter-H)
MIM(needed to config the HMIM-Adapter)	Ethernet interface modules: 1-port 10M/100M Ethernet electrical MIM interface module (RJ45) (MIM-1FE) 2-port 10M/100M Ethernet electrical MIM interface module (RJ45) (MIM-2FE) 4-port 10M/100M Ethernet electrical MIM interface module (RJ45) (MIM-4FE) 1-port 1000M Ethernet electrical MIM interface module (RJ45) (MIM-1GBE) 2-port 1000M Ethernet electrical MIM interface module (RJ45) (MIM-2GBE) 1-port 1000M Ethernet electrical MIM interface module (RJ45) (MIM-1GEF) 2-port 1000M Ethernet electrical MIM interface module (RJ45) (MIM-2GEF) WAN interface modules: 2 channel enhanced synchronous/asynchronous interface module (MIM-2SAE) 4 channel enhanced synchronous/asynchronous interface module (MIM-4SAE) 8 channel enhanced synchronous/asynchronous interface module (MIM-8SAE) 8 port asynchronous serial interface panel (RJ45) (MIM-8ASE) 16 port asynchronous serial interface panel (RJ45) (MIM-16ASE) 1 port CE1/PRI interface module (MIM-1E1) 2 port CE1/PRI interface module (MIM-2E1) 4 port CE1/PRI interface module (MIM-4E1) 8 port E1 interface module (75ohm) (MIM-8E1 (75)) 1-port fractional E1 interface module (MIM-1E1-F) 2-port fractional E1 interface module (MIM-2E1-F) 4-port fractional E1 interface module (MIM-4E1-F) 8 port E1 interface module (75ohm) (MIM-8E1 (75)-F) 2 port CT1/PRI interface module (MIM-2T1) 8 port T1 interface module (MIM-8T1) 2-port fractional T1 interface module MIM-2T1-F) 4-port fractional T1 interface module MIM-4T1-F) 8-port fractional T1 interface module MIM-8T1-F) 1-port T3/CT3 compatible interface module (MIM-1CT3-V2) 1-port T3/CT3 compatible interface module (MIM-1CE3-V2) 1-port SDH/SONET interface module (MIM-1POS-V2) 1-port dual-pair G.SHDSL interface module (MIM-1SHL-4W) - HPE MSR OAP MIM Module with VMware vSphere (JG532A) Voice interface modules: 1 channel E1 voice MIM interface module (MIM-1VE1) 1 channel T1 voice MIM interface module (MIM-1VT1) 2 channel E1 voice MIM interface module (MIM-2VE1) 2 channel T1 voice MIM interface module (MIM-2VT1) 4-port voice module subscriber circuit interface board (MIM-4FXS) 2-port voice module FXO interface module (MIM-2FXO) 4-port voice module FXO interface module (MIM-4FXO)

	8-port voice module FXS-FXO interface module (MIM-8FXS-8FXO) 4 channel voice processing board E&M trunk interface module (MIM-4EM) 4-port ISDN BRI S/T voice interface card (MIM-4BSV) 16-port voice module subscriber circuit interface board (MIM-16FXS)

Table 22 Sierra Modem Module and Host/card compatibility matrix

HPE description	Product code	Module name
HPE MSR 4G LTE SIC Mod for Verizon	JG742A	Sierra-MC7750
HPE MSR 4G LTE SIC Mod for ATT	JG743A	Sierra-MC7700
HPE MSR 4G LTE SIC Mod for Global	JG744A	Sierra-MC7710



CAUTION:

The support and restriction of modules on HPE FlexNetwork MSR Routers Interface Configuration Guide(V7), Appendix Purchase Guide.

Software features

Table 23 MSR Series routers software features

Category	Features
LAN protocol:	ARP (proxy ARP, free ARP, authorization ARP) Ethernet_II Ethernet_SNAP VLAN (PORT-BASED VLAN/MAC-BASED VLAN/VLAN-BASED PORT ISOLATE/VLAN VPN) 802.3x LACP(802.3ad) 802.1p 802.1Q 802.1x QinQ RSTP(802.1w) MSTP(802.1s) GVRP PORT MULTICAST suppression EVI VXLAN
WAN protocols:	PPP PPPoE Client DCC, Dialer Watch ISDN Modem 3G/4G FR

IP services	Fast forwarding (unicast/multicast) TCP UDP IP Option IP unnumber Policy-based routing (unicast or multicast)
Non-IP services:	Netstream
IP application	Ping and Trace DHCP Server DHCP Client DNS client DNS Static DNS proxy DDNS NQA NTP Telnet TFTP Client FTP Client FTP Server
IP route	Static routing management Dynamic routing protocols: • RIP • OSPF • BGP • IS-IS Multicast routing protocols: • IGMP • PIM-DM • PIM-SM • MBGP • MSDP Routing policy
MPLS	LDP LSPM MPLS TE MPLS FW MPLS/BGP VPN VPLS
IPv6	IPv6 basic functions IPv6 ND IPv6 PMTU IPv6 FIB IPv6 ACL IPv6 transition technologies NAT-PT

	IPv6 tunneling 6PE, 6VPE IPv6 routing IPv6 static routing management Multicast routing protocols: • MLD • PIM-DM • PIM-SM • PIM-SSM
AAA	Local authentication Radius HWTacacs LDAP
Firewall	ASPF ACL FILTER Security zone-based firewall
Security	Port security IPSec PORTAL L2TP NAT/NAPT/NAT66 PKI RSA SSH V1.5/2.0 URPF GRE
Reliability	VRRP Backup center BFD IRF Track
L2 QoS	LR Flow-base QOS Policy Port-Based Mirroring Packet Remarking Priority Mapping Port Trust Mode Port Priority Flow Filter FlowControl ACL
Traffic supervision	CAR (Committed Access Rate) LR (Line Rate)
Congestion management	FIFO, PQ, CQ, WFQ, CBQ, RTPQ

Congestion avoidance	WRED/RED
Traffic shaping	GTS (Generic Traffic Shaping)
Other QOS technologies	MPLS QOS cRTP/IPHC Sub-interface QOS
Voice Interfaces	FXS FXO E&M E1VI/T1VI BSV
Voice Signaling	R2 DSS1
SIP	SIP SIP Operation
Codec	G.711A law G.711U law G.723R53 G.723R63 G.729a G.729R8 G.729bR8
Media Process	RTP
Network management	SNMP V1/V2c/V3 MIB SYSLOG RMON NETCONF Information center SMS-based automatic configuration USB-based automatic configuration Web-based network management EAA
Local management	Command line management License management File system management Auto-configure Dual Image
User access management	Console interface login AUX interface login TTY interface login Telnet (VTY) login SSH login FTP login XMODEM

Appendix B Upgrading software

This section describes how to upgrade system software while the router is operating normally or when the router cannot correctly start up.

Software types

The following software types are available:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load application software and the startup configuration file or manage files when the device cannot correctly start up.
- **Comware image**—Includes the following image subcategories:
 - **Boot image**—A .bin file that contains the Linux operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
 - **System image**—A .bin file that contains the minimum feature modules required for device operation and some basic features, including device management, interface management, configuration management, and routing. To have advanced features, you must purchase feature packages.
 - **Feature package**—Includes a set of advanced software features. Users purchase feature packages as needed.
 - **Patch packages**—Irregularly released packages for fixing bugs without rebooting the device. A patch package does not add new features or functions.

Comware software images that have been loaded are called "current software images."

Comware images specified to load at the next startup are called "startup software images."

Boot ROM image, boot image, and system image are required for the system to work. These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images and sets them as startup software images.

Upgrade methods

You can upgrade system software by using one of the following methods:

Upgrade method	Remarks
Centralized devices upgrading from the CLI	You must reboot the router to complete the upgrade. This method can interrupt ongoing network services.
Distributed devices upgrading from the CLI	You must reboot the router to complete the upgrade. This method can interrupt ongoing network services.
Distributed devices ISSU	This method upgrades the router with the least amount of downtime.

Upgrade method	Remarks
Managing files from the BootWare menu	Use this method when the router cannot correctly start up.

Preparing for the upgrade

Before you upgrade system software, complete the following tasks:

- Set up the upgrade environment as shown in [Table 25](#).
- Configure routes to make sure that the router and the file server can reach each other.
- Run a TFTP, FTP or SFTP server on the file server.
- Log in to the CLI of the router through the console port.
- Copy the upgrade file to the file server and correctly set the working directory on the TFTP, FTP or SFTP server.
- Make sure the upgrade has minimal impact on the network services. During the upgrade, the router cannot provide any services.



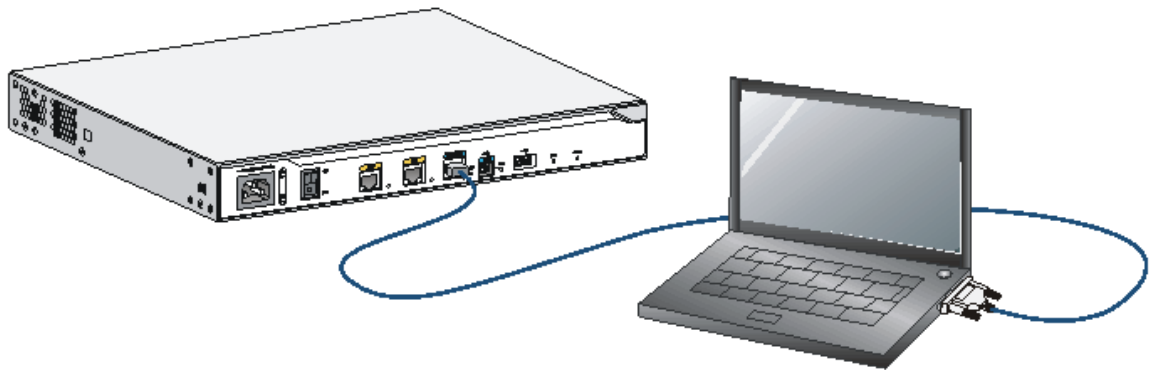
IMPORTANT:

In the BootWare menu, if you choose to download files over Ethernet, the Ethernet port must be GE0 on an MSR954P, MSR958, MSR2003, MSR2004-24, MSR2004-48, MSR3012, MSR3024, MSR3044, and MSR3064 router, and must be M-GE0 on an MSR4060 and MSR4080 router.

Table 24 Storage media

Model	Storage medium	Path	Router Types
MSR2003	Flash	flash:/	Centralized devices
MSR2004-24	Flash	flash:/	Centralized devices
MSR2004-48	Flash	flash:/	Centralized devices
MSR3012	CF card	cfa0:/	Centralized devices
MSR3024	CF card	cfa0:/	Centralized devices
MSR3044	CF card	cfa0:/	Centralized devices
MSR3064	CF card	cfa0:/	Centralized devices
MSR4060	CF card	cfa0:/	Centralized devices
MSR4080	CF card	cfa0:/	Distributed devices
MSR954P	Flash	flash:/	Centralized devices
MSR958	Flash	flash:/	Centralized devices

Figure 1 Set up the upgrade environment



Centralized devices upgrading from the CLI

You can use the TFTP, FTP or SFTP commands on the router to access the TFTP,FTP or SFTP server to back up or download files.

Saving the running configuration and verifying the storage space

1. Save the running configuration

```
<HPE>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Configuration is saved to device successfully.
<HPE>
```

2. Identify the system software image and configuration file names and verify that the cfa0 has sufficient space for the new system software image.

```
<HPE>dir
Directory of cfa0: (VFAT)
 0 -rw-      3902 Nov 28 2021 13:16:10  B64D065SP12_info.txt
 1 -rw-      5853 Jan 28 2022 15:55:50  B64D065SP14_info.txt
 2 -rw-      1939 Dec 31 2021 18:53:26  B64D076SP02_info.txt
 3 -rw-      1908 Nov 29 2021 20:17:36  B64D078_info.txt
 4 -rw-      1908 Jan 25 2022 16:53:18  B64D080_info.txt
 5 drw-          - Nov 28 2020 20:50:52  Eagle
 6 -rw-      2578 May 31 2021 05:46:56  aaa.cfg
 7 -rw-     79820 May 31 2021 05:46:58  aaa.mdb
 8 -rw-      2870 Jan 04 2022 23:31:28  atfinitia.cfg
 9 -rw-     81488 Jan 04 2022 23:31:30  atfinitia.mdb
10 drw-          - Jan 12 2022 05:05:08  diagfile
11 -rw-       140 Jan 28 2022 15:41:42  ifindex.dat
12 -rw-       288 Jan 25 2022 16:45:30  lauth.dat
13 -rw-    81034 Sep 11 2020 05:51:26  ldp.mdb
```

```

14 drw-          - Feb 14 2020 17:07:26 license
15 drw-          - Oct 27 2021 15:32:46 logfile
16 -rw-      9004032 Jan 28 2022 15:42:34 msr3000-cmw710-boot-r6728p25.bin
17 -rw-      3781632 Jan 28 2022 15:44:06 msr3000-cmw710-data-r6728p25.bin
18 -rw-      547840 Jan 28 2022 15:44:04 msr3000-cmw710-security-r6728p25.bin
19 -rw-      91685888 Jan 28 2022 15:43:46 msr3000-cmw710-system-r6728p25.bin
20 -rw-      1299456 Jan 28 2022 15:44:04 msr3000-cmw710-voice-r6728p25.bin
21 -rw-    106327040 Jan 28 2022 15:33:54 msr3000.ipe
22 -rw-          2692 Dec 24 2021 08:47:28 mytest.cfg
23 drw-          - Mar 09 2021 07:52:50 pkey
24 drw-          - Jan 04 2022 23:16:38 pki
25 drw-          - Aug 26 2020 00:33:28 seclog
26 -rw-          2815 Jan 28 2022 15:41:44 startup.cfg
27 -rw-      70179 Jan 28 2022 15:41:44 startup.mdb
28 -rw-      2973 Jun 22 2007 17:55:40 startup1.cfg
29 -rw-      69859 Jun 22 2007 17:55:40 startup1.mdb
30 -rw-      3036 Jun 22 2007 17:55:52 startup2.cfg
31 -rw-      69920 Jun 22 2007 17:55:52 startup2.mdb
32 -rw-      4242 Mar 09 2021 08:01:16 startup4.cfg
33 -rw-      88077 Mar 09 2021 08:01:16 startup4.mdb
34 -rw-      79765 Nov 11 2020 02:22:40 test.mdb
35 -rw-      79765 Nov 11 2020 01:24:02 test2.mdb
36 -rw-      87512 Mar 08 2021 20:10:00 ttt2.mdb

```

252164 KB total (38888 KB free)

<HPE>

Downloading the image file to the router

Using TFTP

Download the system software image file, for example, msr2000.ipe to the cfa0 on the router.

```

<HPE>tftp 192.168.1.100 get msr3000.ipe
  % Total      % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload    Total   Spent    Left   Speed
100 35.9M  100 35.9M    0     0   559k      0  0:01:05  0:01:05 --:--:--  546k

```

<HPE>

Using FTP

1. From FTP client view, download the system software image file (for example, msr2000.ipe) to the CF card on the router.

```

ftp> get msr3000.ipe
msr3000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)

```

- ```
[ftp]
```
2. Return to user view.
- ```
[ftp]quit
221 Service closing control connection
```

<HPE>

Using SFTP

1. From SFTP client view, download the system software image file (for example, msr2000.ipe) to the CF card on the router.

```
sftp-client> get msr3000.ipe
msr3000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)
```

```
sftp-client>
```

2. Return to user view.

```
sftp-client> quit
221 Service closing control connection
```

<HPE>

Specifying the startup image file

1. Specify the msr3000.ipe file as the main image file at the next reboot.

```
<HPE>boot-loader file cfa0:/msr3000.ipe main
Verifying the file cfa0:/msr3000.ipe on the
device.....Done.
HPE MSR3012 images in IPE:
  msr3000-cmw710-boot-r6728p25.bin
  msr3000-cmw710-system-r6728p25.bin
  msr3000-cmw710-security-r6728p25.bin
  msr3000-cmw710-voice-r6728p25.bin
  msr3000-cmw710-data-r6728p25.bin
This command will set the main startup software images. Please do not reboot the device
during the upgrade. Continue? [Y/N]:y
Add images to the device.
File cfa0:/msr3000-cmw710-boot-r6728p25.bin already exists on the device.
File cfa0:/msr3000-cmw710-system-r6728p25.bin already exists on the device.
File cfa0:/msr3000-cmw710-security-r6728p25.bin already exists on the device.
File cfa0:/msr3000-cmw710-voice-r6728p25.bin already exists on the device.
File cfa0:/msr3000-cmw710-data-r6728p25.bin already exists on the device.
Overwrite the existing files?[Y/N]:y
Decompressing file msr3000-cmw710-boot-r6728p25.bin to
cfa0:/msr3000-cmw710-boot-r6728p25.bin.....Done.
Decompressing file msr3000-cmw710-system-r6728p25.bin to
cfa0:/msr3000-cmw710-system-r6728p25.bin.....
.....Done.
```



```
Decompressing file msr3000-cmw710-security-r6728p25.bin to
cfa0:/msr3000-cmw710-security-r6728p25.bin...Done.
Decompressing file msr3000-cmw710-voice-r6728p25.bin to
cfa0:/msr3000-cmw710-voice-r6728p25.bin...Done.
Decompressing file msr3000-cmw710-data-r6728p25.bin to
cfa0:/msr3000-cmw710-data-r6728p25.bin.....Done.
Verifying the file cfa0:/msr3000-cmw710-boot-r6728p25.bin on the device....Done.
Verifying the file cfa0:/msr3000-cmw710-system-r6749P14.bin on the
device.....Done.
Verifying the file cfa0:/msr3000-cmw710-security-r6749P14.bin on the device...Done.
Verifying the file cfa0:/msr3000-cmw710-voice-r6749P14.bin on the device...Done.
Verifying the file cfa0:/msr3000-cmw710-data-r6749P14.bin on the device...Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on the device.
```

<HPE>

2. Verify that the file has been loaded.

```
<HPE> display boot-loader
Software images on the device:
Current software images:
  cfa0:/msr3000-cmw710-boot-r6749P14.bin
  cfa0:/msr3000-cmw710-system-r6749P14.bin
  cfa0:/msr3000-cmw710-security-r6749P14.bin
  cfa0:/msr3000-cmw710-voice-r6749P14.bin
  cfa0:/msr3000-cmw710-data-r6749P14.bin
Main startup software images:
  cfa0:/msr3000-cmw710-boot-r6749P14.bin
  cfa0:/msr3000-cmw710-system-r6749P14.bin
  cfa0:/msr3000-cmw710-security-r6749P14.bin
  cfa0:/msr3000-cmw710-voice-r6749P14.bin
  cfa0:/msr3000-cmw710-data-r6749P14.bin
Backup startup software images:
  None
<HPE>
```

Rebooting and completing the upgrade

1. Reboot the router.

```
<HPE>reboot
Start to check configuration with next startup configuration file, please
wait.....DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
<HPE>
System is starting...
```

2. After the reboot is complete, verify that the system software image is correct.

```
<HPE> display version
HPE Comware Software, Version 7.1.064, Release 6749P14
Copyright (c) 2010-2022 Hewlett Packard Enterprise Development LP
```

```

HPE MSR3012 uptime is 0 weeks, 0 days, 0 hours, 2 minutes
Last reboot reason : User reboot
Boot image: cfa0:/msr3000-cmw710-boot-r6749P14.bin
Boot image version: 7.1.064P80, Release 6749P14
Compiled Jun 16 2022 15:00:00
System image: cfa0:/msr3000-cmw710-system-r6749P14.bin
System image version: 7.1.064, Release 6749P14
Compiled Jun 16 2022 15:00:00
Feature image(s) list:
cfa0:/msr3000-cmw710-security-r6749P14.bin, version: 7.1.064
Compiled Jun 16 2022 15:00:00
cfa0:/msr3000-cmw710-voice-r6749P14.bin, version: 7.1.064
Compiled Jun 16 2022 15:00:00
cfa0:/msr3000-cmw710-data-r6749P14.bin, version: 7.1.064
Compiled Jun 16 2022 15:00:00

```

```

CPU ID: 0x2
1G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB                Version: 2.0
CPLD                Version: 2.0
Basic BootWare Version: 1.82
Extended BootWare Version: 1.82

[ SLOT 0]AUX                (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[ SLOT 0]GE0/0              (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[ SLOT 0]GE0/1              (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[ SLOT 0]GE0/2              (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[ SLOT 0]CELLULAR0/0        (Hardware)2.0, (Driver)1.0, (CPLD)2.0
[ SLOT 0]CELLULAR0/1        (Hardware)2.0, (Driver)1.0, (CPLD)2.0

```

<HPE>

Distributed devices upgrading from the CLI

You can use the TFTP, FTP or SFTP commands on the router to access the TFTP,FTP or SFTP server to back up or download files.

Display the slot number of the active MPU

Perform the **display device** command in any view to display the slot number of the active MPU. By default, the standby MPU will automatically synchronize the image files from active MPU.

<HPE>display device

Slot No.	Board Type	Status	Primary	SubSlots
0	MPU-100	Normal	Master	0
1	MPU-100	Normal	Standby	0
2	SPU-100	Normal	N/A	10

<HPE>

Save the current configuration and verify the storage space

1. Perform the **save** command in any view to save the current configuration.

```
<HPE>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Configuration is saved to device successfully.
<HPE>
```

2. Perform the **dir** command in user view to identify the system software image and configuration file names and verify that the CF card has sufficient space for the new system software image.

```
<HPE>dir
Directory of cfa0:
 0 drw-          - Jan 07 2021 14:02:12   diagfile
 1 -rw-          307 Jan 22 2021 17:02:02   ifindex.dat
 2 drw-          - Jan 07 2021 14:02:12   license
 3 drw-          - Jan 22 2021 13:42:00   logfile
 4 -rw-        21412864 Jan 22 2021 16:49:00  MSR4000-cmw710-boot-r6749P14.bin
 5 -rw-        1123328 Jan 22 2021 16:50:30  MSR4000-cmw710-data-r6749P14.bin
 6 -rw-         11264 Jan 22 2021 16:50:26  MSR4000-cmw710-security-r6749P14.bin
 7 -rw-       45056000 Jan 22 2021 16:49:34  MSR4000-cmw710-system-r6749P14.bin
 8 -rw-       2746368 Jan 22 2021 16:50:26  MSR4000-cmw710-voice-r6749P14.bin
 9 drw-          - Jan 07 2021 14:02:12   seclog
10 -rw-          2166 Jan 22 2021 17:02:02   startup.cfg
11 -rw-         34425 Jan 22 2021 17:02:02   startup.mdb

507492 KB total (438688 KB free)

<HPE>
```

Download the image file to the router

Using TFTP

Perform the **tftp get** command in user view to download the system software image file, for example, msr4000.ipe to the CF card on the router.

```
<HPE>tftp 192.168.1.100 get msr4000.ipe
% Total      % Received % Xferd  Average Speed   Time    Time       Time  Current
                                 Dload  Upload    Total   Spent    Left   Speed
 45 67.0M    45 30.4M    0     0   792k      0  0:01:26  0:00:39  0:00:47  844k
100 67.0M   100 67.0M    0     0   772k      0  0:01:28  0:01:28  --:--:--  745k
<HPE>
```

Using FTP

1. Perform the **get** command in FTP client view to download the system software image file msr4000.ipe to the CF card on the router.

```
ftp> get msr4000.ipe
msr4000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
```

```

125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)
[ftp]

```

2. Perform the **quit** command in FTP client view to return to user view.

```

[ftp]quit
221 Service closing control connection
<HPE>

```

Using SFTP

1. From SFTP client view, download the system software image file (for example, msr4000.ipe) to the CF card on the router.

```

sftp-client> get msr4000.ipe
msr4000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)

```

```

sftp-client>

```

2. Return to user view.

```

sftp-client>quit
221 Service closing control connection
<HPE>

```

Copy the image file to CF card root directory of the standby MPU

```

<HPE> copy msr4000.ipe slot1#cfa0:/
Copy cfa0:/msr4000.ipe to slot1#cfa0:/msr4000.ipe?[Y/N]:y
Copying file cfa0:/msr4000.ipe to slot1#cfa0:/ msr4000.ipe...Done.

```

Specifying the startup image file

1. Perform the **boot-loader** command in user view to specify the msr4000.ipe file as the main image file for the active MPU on slot 0 at the next reboot.

```

<HPE>boot-loader file cfa0:/msr4000.ipe slot 0 main
Images in IPE:
  msr4000-cmw710-boot-r6749P14.bin
  msr4000-cmw710-system-r6749P14.bin
  msr4000-cmw710-security-r6749P14.bin
  msr4000-cmw710-voice-r6749P14.bin
  msr4000-cmw710-data-r6749P14.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to the device.
Successfully copied cfa0:/msr4000-cmw710-boot-r6749P14.bin to
cfa0:/msr4000-cmw710-boot-r6749P14.bin.
Successfully copied cfa0:/msr4000-cmw710-system-r6749P14.bin to
cfa0:/msr4000-cmw710-system-r6749P14.bin.
Successfully copied cfa0:/msr4000-cmw710-security-r6749P14.bin to
cfa0:/msr4000-cmw710-security-r6749P14.bin.

```

Successfully copied cfa0:/msr4000-cmw710-voice-r6749P14.bin to
cfa0:/msr4000-cmw710-voice-r6749P14.bin.

Successfully copied cfa0:/msr4000-cmw710-data-r6749P14.bin to
cfa0:/msr4000-cmw710-data-r6749P14.bin.

The images that have passed all examinations will be used as the main startup software
images at the next reboot on the device.

<HPE>

2. Perform the **boot-loader** command in user view to specify the msr4000.ipe file as the main image file for the standby MPU on slot 1 at the next reboot.

<HPE>boot-loader file cfa0:/msr4000.ipe slot 0 main

Images in IPE:

msr4000-cmw710-boot-r6749P14.bin
msr4000-cmw710-system-r6749P14.bin
msr4000-cmw710-security-r6749P14.bin
msr4000-cmw710-voice-r6749P14.bin
msr4000-cmw710-data-r6749P14.bin

This command will set the main startup software images. Continue? [Y/N]:y

Add images to the device.

Successfully copied cfa0:/msr4000-cmw710-boot-r6749P14.bin to
cfa0:/msr4000-cmw710-boot-r6749P14.bin.

Successfully copied cfa0:/msr4000-cmw710-system-r6749P14.bin to
cfa0:/msr4000-cmw710-system-r6749P14.bin.

Successfully copied cfa0:/msr4000-cmw710-security-r6749P14.bin to
cfa0:/msr4000-cmw710-security-r6749P14.bin.

Successfully copied cfa0:/msr4000-cmw710-voice-r6749P14.bin to
cfa0:/msr4000-cmw710-voice-r6749P14.bin.

Successfully copied cfa0:/msr4000-cmw710-data-r6749P14.bin to
cfa0:/msr4000-cmw710-data-r6749P14.bin.

The images that have passed all examinations will be used as the main startup software
images at the next reboot on the device.

<HPE>

3. Perform the **display boot-loader** command in user view to verify that the file has been loaded.

<HPE> display boot-loader

Software images on slot 0:

Current software images:

cfa0:/MSR4000-cmw710-boot-r6749P14.bin
cfa0:/MSR4000-cmw710-system-r6749P14.bin
cfa0:/MSR4000-cmw710-security-r6749P14.bin
cfa0:/MSR4000-cmw710-voice-r6749P14.bin
cfa0:/MSR4000-cmw710-data-r6749P14.bin

Main startup software images:

cfa0:/MSR4000-cmw710-boot-r6749P14.bin
cfa0:/MSR4000-cmw710-system-r6749P14.bin
cfa0:/MSR4000-cmw710-security-r6749P14.bin
cfa0:/MSR4000-cmw710-voice-r6749P14.bin
cfa0:/MSR4000-cmw710-data-r6749P14.bin

Backup startup software images:

None

Software images on slot 1:

Current software images:

```
cfa0:/MSR4000-cmw710-boot-r6749P14.bin
cfa0:/MSR4000-cmw710-system-r6749P14.bin
cfa0:/MSR4000-cmw710-security-r6749P14.bin
cfa0:/MSR4000-cmw710-voice-r6749P14.bin
cfa0:/MSR4000-cmw710-data-r6749P14.bin
```

Main startup software images:

```
cfa0:/MSR4000-cmw710-boot-r6749P14.bin
cfa0:/MSR4000-cmw710-system-r6749P14.bin
cfa0:/MSR4000-cmw710-security-r6749P14.bin
cfa0:/MSR4000-cmw710-voice-r6749P14.bin
cfa0:/MSR4000-cmw710-data-r6749P14.bin
```

Backup startup software images:

None

Reboot and completing the upgrade

1. Perform the **reboot** command in user view to reboot the router.

```
<HPE>reboot
Start to check configuration with next startup configuration file, please
wait.....DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
<HPE>
System is starting..
```

2. After the reboot is complete, perform the **display version** command to verify that the system software image is correct.

```
<HPE> display version
HPE Comware Software, Version 7.1.042, Release 0821P10
Copyright (c) 2010-2021 Hewlett-Packard Development Company, L.P.
HPE MSR4060 uptime is 0 weeks, 0 days, 11 hours, 49 minutes
Last reboot reason : Power on
Boot image: cfa0:/MSR4000-cmw710-boot-r6749P14.bin
Boot image version: 7.1.040, Alpha 0821
System image: cfa0:/MSR4000-cmw710-system-r6749P14.bin
System image version: 7.1.040, Alpha 0821
Feature image(s) list:
  cfa0:/MSR4000-cmw710-security-r6749P14.bin, version: 7.1.040
  cfa0:/MSR4000-cmw710-voice-r6749P14.bin, version: 7.1.040
  cfa0:/MSR4000-cmw710-data-r6749P14.bin, version: 7.1.040

Slot 0: MPU-100 uptime is 0 week, 0 day, 1 hour, 20 minutes
Last reboot reason : Power on
CPU ID: 0x3
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB                Version: 2.0
CPLD                Version: 1.0
Basic   BootWare Version: 1.04
Extended BootWare Version: 1.04
```

[SUBSLOT 0]CON	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]AUX	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]MGEO	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0

Slot 1: MPU-100 uptime is 0 week, 0 day, 1 hour, 8 minutes

Last reboot reason : User reboot

CPU ID: 0x3

2G bytes DDR3 SDRAM Memory

8M bytes Flash Memory

PCB Version: 2.0

CPLD Version: 1.0

Basic BootWare Version: 1.05

Extended BootWare Version: 1.05

[SUBSLOT 0]CON	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]AUX	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]MGEO	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0

Slot 2: SPU-100 uptime is 0 week, 0 day, 1 hour, 19 minutes

Last reboot reason : Power on

CPU ID: 0x5

2G bytes DDR3 SDRAM Memory

8M bytes Flash Memory

PCB Version: 2.0

CPLD Version: 1.0

Basic BootWare Version: 1.02

Extended BootWare Version: 1.02

[SUBSLOT 0]GE2/0/0	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]GE2/0/1	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]GE2/0/2	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]GE2/0/3	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]CELLULAR2/0/0	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 0]CELLULAR2/0/1	(Hardware)2.0	(Driver)1.0,	(Cpld)1.0
[SUBSLOT 1]HMIM-4SAE	(Hardware)3.0	(Driver)1.0,	(Cpld)4.0

Distributed devices ISSU

The In-Service Software Upgrade (ISSU) function enables software upgrade with the least amount of downtime.

To implement ISSU of a distributed device, use these guidelines:

- Make sure the device has two MPUs.
- Upgrade the standby MPU is upgraded first to form a new forwarding plane and a new control plane.
- Upgrade the active MPU after the standby MPU operates correctly. The standby MPU will synchronize data and configuration from the active MPU and take over the forwarding and control functions.

Disabling the standby MPU auto-update function

When you upgrade the active MPU of a dual-MPU distributed device, the standby MPU auto-update function automatically upgrades the standby MPU by default. To use ISSU, you must disable the function.

To disable the standby MPU auto-update function:

1. View the roles of the MPUs.

```
<HPE>display device
```

Slot No.	Board Type	Status	Primary	SubSlots
0	MPU-100	Normal	Master	0
1	MPU-100	Normal	Standby	0
2	SPU-100	Normal	N/A	10

```
<HPE>
```

The output shows that the MPU in slot 0 is the active MPU.

2. Disable the standby MPU auto-update function.

```
<HPE>system-view
[Sysname]version check ignore
[Sysname]undo version auto-update enable
```

Saving the running configuration and verifying the storage space

1. Save the running configuration.

```
<HPE>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Configuration is saved to device successfully.
<HPE>
```

2. Check the storage space.

```
<HPE>dir
Directory of cfa0:
 0 drw-          - Jan 07 2021 14:02:12  diagfile
 1 -rw-          307 Jan 22 2021 17:02:02  ifindex.dat
 2 drw-          - Jan 07 2021 14:02:12  license
 3 drw-          - Jan 22 2021 13:42:00  logfile
 4 -rw-      20050944 Jan 10 2021 09:06:48  msr4000-cmw710-boot-r6749P14.bin
 5 -rw-      2001920 Jan 10 2021 09:08:28  msr4000-cmw710-data-r6749P14.bin
 6 -rw-      11264 Jan 10 2021 09:08:18  msr4000-cmw710-security-r6749P14.bin
 7 -rw-     61538304 Jan 10 2021 09:07:36  msr4000-cmw710-system-r6749P14.bin
 8 -rw-      3232768 Jan 10 2021 09:08:22  msr4000-cmw710-voice-r6749P14.bin
 9 drw-          - Jan 07 2021 14:02:12  seclog
10 -rw-          2166 Jan 22 2021 17:02:02  startup.cfg
11 -rw-      34425 Jan 22 2021 17:02:02  startup.mdb
```



```
507492 KB total (438688 KB free)
```

```
<HPE>
```

The output shows the CF card has 438688 KB of free storage space. If the CF card of your device is not sufficient for the upgrade image, delete unused files.

Downloading the upgrade image file to the router

Using TFTP

Download the upgrade image file (for example, msr4000.ipe) to the CF card on the router.

```
<HPE>tftp 192.168.1.100 get msr4000.ipe
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
45 67.0M	45 30.4M	0	0	792k	0	0:01:26 0:00:39 0:00:47	844k
100 67.0M	100 67.0M	0	0	772k	0	0:01:28 0:01:28 --:--:--	745k

```
<HPE>
```

Using FTP

1. From FTP client view, download the upgrade image file (for example, msr4000.ipe) to the CF card on the router.

```
ftp> get msr4000.ipe
msr4000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)
[ftp]
```

2. Return to user view.

```
[ftp]quit
221 Service closing control connection
<HPE>
```

Using SFTP

1. From SFTP client view, download the upgrade image file (for example, msr4000.ipe) to the CF card on the router.

```
sftp-client> get msr4000.ipe
msr4000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)
```

```
sftp-client>
```

2. Return to user view.

```
sftp-client>quit
221 Service closing control connection
<HPE>
```

Copying the image file to the root directory of the CF card on the standby MPU

```
<HPE> copy msr4000.ipe slot1#cfa0:/
```

```
Copy cfa0:/msr4000.ipe to slot1#cfa0:/msr4000.ipe?[Y/N]:y
Copying file cfa0:/msr4000.ipe to slot1#cfa0:/ msr4000.ipe...Done.
```

Upgrading the standby MPU

1. Specify the msr4000.ipe file as the main startup image file for the standby MPU.

```
<HPE>boot-loader file msr4000.ipe slot 1 main
Verifying the IPE file and the images.....Done.
HPE MSR4060 images in IPE:
    msr4000-cmw710-boot-r6749P14.bin
    msr4000-cmw710-system-r6749P14.bin
    msr4000-cmw710-security-r6749P14.bin
    msr4000-cmw710-voice-r6749P14.bin
    msr4000-cmw710-data-r6749P14.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
Decompressing file msr4000-cmw710-boot-r6749P14.bin to
slot1#cfa0:/msr4000-cmw710-boo
t-r6749P14.bin.....Done.
Decompressing file msr4000-cmw710-system-r6749P14.bin to
slot1#cfa0:/msr4000-cmw710-s
ystem-r6749P14.bin.....Done.
Decompressing file msr4000-cmw710-security-r6749P14.bin to
slot1#cfa0:/msr4000-cmw710
-security-r6749P14.bin...Done.
Decompressing file msr4000-cmw710-voice-r6749P14.bin to
slot1#cfa0:/msr4000-cmw710-vo
ice-r6749P14.bin....Done.
Decompressing file msr4000-cmw710-data-r6749P14.bin to
slot1#cfa0:/msr4000-cmw710-dat
a-r6749P14.bin...Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 1.
```

2. Reboot the standby MPU.

```
<HPE>reboot slot 1
This command will reboot the specified slot, Continue? [Y/N]:y
Now rebooting, please wait...
```

3. After the standby MPU starts up, verify the startup image files.

```
<HPE>display boot-loader
Software images on slot 0:
Current software images:
    cfa0:/msr4000-cmw710-boot-r6749P14.bin
    cfa0:/msr4000-cmw710-system-r6749P14.bin
    cfa0:/msr4000-cmw710-security-r6749P14.bin
    cfa0:/msr4000-cmw710-voice-r6749P14.bin
    cfa0:/msr4000-cmw710-data-r6749P14.bin
Main startup software images:
    cfa0:/msr4000-cmw710-boot-r6749P14.bin
    cfa0:/msr4000-cmw710-system-r6749P14.bin
```

```
cfa0:/msr4000-cmw710-security-r6749P14.bin
cfa0:/msr4000-cmw710-voice-r6749P14.bin
cfa0:/msr4000-cmw710-data-r6749P14.bin
```

Backup startup software images:

```
cfa0:/msr4000-cmw710-boot-r6749P14.bin
cfa0:/msr4000-cmw710-system-r6749P14.bin
cfa0:/msr4000-cmw710-security-r6749P14.bin
cfa0:/msr4000-cmw710-voice-r6749P14.bin
cfa0:/msr4000-cmw710-data-r6749P14.bin
```

Software images on slot 1:

Current software images:

```
cfa0:/msr4000-cmw710-boot-r6749P14.bin
cfa0:/msr4000-cmw710-system-r6749P14.bin
cfa0:/msr4000-cmw710-security-r6749P14.bin
cfa0:/msr4000-cmw710-voice-r6749P14.bin
cfa0:/msr4000-cmw710-data-r6749P14.bin
```

Main startup software images:

```
cfa0:/msr4000-cmw710-boot-r6749P14.bin
cfa0:/msr4000-cmw710-system-r6749P14.b3000in
cfa0:/msr4000-cmw710-security-r6749P14.bin
cfa0:/msr4000-cmw710-voice-r6749P14.bin
cfa0:/msr4000-cmw710-data-r6749P14.bin
```

Backup startup software images:

```
cfa0:/msr4000-cmw710-boot-r6749P14.bin
cfa0:/msr4000-cmw710-system-r6749P14.bin
cfa0:/msr4000-cmw710-security-r6749P14.bin
cfa0:/msr4000-cmw710-voice-r6749P14.bin
cfa0:/msr4000-cmw710-data-r6749P14.bin
```

The output shows that the standby MPU is running the new images.

Upgrading the active MPU

1. Specify the msr4000.ipe file as the main startup image file for the active MPU.

```
<HPE>boot-loader file msr4000.ipe slot 0 main
```

Verifying the IPE file and the images.....Done.

HPE MSR4060 images in IPE:

```
msr4000-cmw710-boot-r6749P14.bin
msr4000-cmw710-system-r6749P14.bin
msr4000-cmw710-security-r6749P14.bin
msr4000-cmw710-voice-r6749P14.bin
msr4000-cmw710-data-r6749P14.bin
```

This command will set the main startup software images. Continue? [Y/N]:y

Add images to slot 0.

```
Decompressing file msr4000-cmw710-boot-r6749P14.bin to
cfa0:/msr4000-cmw710-boot-r6749P14.bin.....Done.
```

```
Decompressing file msr4000-cmw710-system-r6749P14.bin to
cfa0:/msr4000-cmw710-system-r6749P14.bin.....
.....Done.
```

```
Decompressing file msr4000-cmw710-security-r6749P14.bin to
cfa0:/msr4000-cmw710-security-r6749P14.bin...Done.
Decompressing file msr4000-cmw710-voice-r6749P14.bin to
cfa0:/msr4000-cmw710-voice-r6749P14.bin....Done.
Decompressing file msr4000-cmw710-data-r6749P14.bin to
cfa0:/msr4000-cmw710-data-r6749P14.bin...Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 0.
```

2. Reboot the active MPU.

```
<HPE>reboot slot 0
This command will reboot the specified slot, Continue? [Y/N]:y
Now rebooting, please wait...
```

The standby MPU takes over the forwarding and controlling functions before the active MPU reboots.

3. After the active MPU starts up, verify the startup image files.

```
<HPE>display boot-loader
Software images on slot 0:
Current software images:
  cfa0:/msr4000-cmw710-boot-r6749P14.bin
  cfa0:/msr4000-cmw710-system-r6749P14.bin
  cfa0:/msr4000-cmw710-security-r6749P14.bin
  cfa0:/msr4000-cmw710-voice-r6749P14.bin
  cfa0:/msr4000-cmw710-data-r6749P14.bin
Main startup software images:
  cfa0:/msr4000-cmw710-boot-r6749P14.bin
  cfa0:/msr4000-cmw710-system-r6749P14.bin
  cfa0:/msr4000-cmw710-security-r6749P14.bin
  cfa0:/msr4000-cmw710-voice-r6749P14.bin
  cfa0:/msr4000-cmw710-data-r6749P14.bin
Backup startup software images:
  cfa0:/msr4000-cmw710-boot-r6749P14.bin
  cfa0:/msr4000-cmw710-system-r6749P14.bin
  cfa0:/msr4000-cmw710-security-r6749P14.bin
  cfa0:/msr4000-cmw710-voice-r6749P14.bin
  cfa0:/msr4000-cmw710-data-r6749P14.bin
Software images on slot 1:
Current software images:
  cfa0:/msr4000-cmw710-boot-r6749P14.bin
  cfa0:/msr4000-cmw710-system-r6749P14.bin
  cfa0:/msr4000-cmw710-security-r6749P14.bin
  cfa0:/msr4000-cmw710-voice-r6749P14.bin
  cfa0:/msr4000-cmw710-data-r6749P14.bin
Main startup software images:
  cfa0:/msr4000-cmw710-boot-r6749P14.bin
  cfa0:/msr4000-cmw710-system-r6749P14.bin
  cfa0:/msr4000-cmw710-security-r6749P14.bin
  cfa0:/msr4000-cmw710-voice-r6749P14.bin
  cfa0:/msr4000-cmw710-data-r6749P14.bin
Backup startup software images:
```

```
cfa0:/msr4000-cmw710-boot-r6749P14.bin
cfa0:/msr4000-cmw710-system-r6749P14.bin
cfa0:/msr4000-cmw710-security-r6749P14.bin
cfa0:/msr4000-cmw710-voice-r6749P14.bin
cfa0:/msr4000-cmw710-data-r6749P14.bin
```

4. Perform the **display boot-loader** command in user view to verify that the file has been loaded.

```
<HPE> display boot-loader
Software images on slot 0:
Current software images:
  cfa0:/MSR4000-cmw710-boot-r6749P14.bin
  cfa0:/MSR4000-cmw710-system-r6749P14.bin
  cfa0:/MSR4000-cmw710-security-r6749P14.bin
  cfa0:/MSR4000-cmw710-voice-r6749P14.bin
  cfa0:/MSR4000-cmw710-data-r6749P14.bin
Main startup software images:
  cfa0:/MSR4000-cmw710-boot-r6749P14.bin
  cfa0:/MSR4000-cmw710-system-r6749P14.bin
  cfa0:/MSR4000-cmw710-security-r6749P14.bin
  cfa0:/MSR4000-cmw710-voice-r6749P14.bin
  cfa0:/MSR4000-cmw710-data-r6749P14.bin
Backup startup software images:
  None
Software images on slot 1:
Current software images:
  cfa0:/MSR4000-cmw710-boot-r6749P14.bin
  cfa0:/MSR4000-cmw710-system-r6749P14.bin
  cfa0:/MSR4000-cmw710-security-r6749P14.bin
  cfa0:/MSR4000-cmw710-voice-r6749P14.bin
  cfa0:/MSR4000-cmw710-data-r6749P14.bin
Main startup software images:
  cfa0:/MSR4000-cmw710-boot-r6749P14.bin
  cfa0:/MSR4000-cmw710-system-r6749P14.bin
  cfa0:/MSR4000-cmw710-security-r6749P14.bin
  cfa0:/MSR4000-cmw710-voice-r6749P14.bin
  cfa0:/MSR4000-cmw710-data-r6749P14.bin
Backup startup software images:
  None
```

Upgrading from the BootWare menu

You can use the following methods to upgrade software from the BootWare menu:

- [Using TFTP/FTP to upgrade software through an Ethernet port](#)
- [Using XMODEM to upgrade software through the console port](#)

Accessing the BootWare menu

1. Power on the router (for example, an HPE MSR 3012 router), and you can see the following information:

```

System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start heavy memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing...Done.

```

```

*****
*
*                      HPE MSR3012 BootWare, Version 1.82
*
*****

```

Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP

```

Compiled Date      : Jul 14 2020
CPU ID            : 0x2
Memory Type       : DDR3 SDRAM
Memory Size       : 1024MB
Flash Size        : 8MB
cfa0 Size         : 247MB
CPLD Version      : 2.0
PCB Version       : 2.0

```

```

BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...

```

2. Press Ctrl + B to access the BootWare menu.

```

Password recovery capability is enabled.
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

```

```

=====<EXTEND-BOOTWARE MENU>=====
|<1> Boot System                                     |
|<2> Enter Serial SubMenu                           |
|<3> Enter Ethernet SubMenu                         |
|<4> File Control                                   |
|<5> Restore to Factory Default Configuration      |
|<6> Skip Current System Configuration              |
|<7> BootWare Operation Menu                       |
|<8> Skip authentication for console login         |
|<9> Storage Device Operation                      |
|<0> Reboot                                         |
=====

```

```

Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9):

```

Table 25 BootWare menu options

Item	Description
<1> Boot System	Boot the system software image.
<2> Enter Serial SubMenu	Access the Serial submenu (see Table 28) for upgrading system software through the console port or changing the serial port settings.
<3> Enter Ethernet SubMenu	Access the Ethernet submenu (see Table 26) for upgrading system software through an Ethernet port or changing Ethernet settings.
<4> File Control	Access the File Control submenu (see Table 29) to retrieve and manage the files stored on the router.
<5> Restore to Factory Default Configuration	Delete the next-startup configuration files and load the factory-default configuration.
<6> Skip Current System Configuration	Start the router with the factory default configuration. This is a one-time operation and does not take effect at the next reboot. You use this option when you forget the console login password.
<7> BootWare Operation Menu	Access the BootWare Operation menu for backing up, restoring, or upgrading BootWare. When you upgrade the system software image, BootWare is automatically upgraded. HPE does not recommend upgrading BootWare separately. This document does not cover using the BootWare Operation menu.
<8> Skip authentication for console login	Clear all the authentication schemes on the console port.
<9> Storage Device Operation	Access the Storage Device Operation menu to manage storage devices. Using this option is beyond this chapter.
<0> Reboot	Restart the router.

Using TFTP/FTP to upgrade software through an Ethernet port

1. Enter **3** in the BootWare menu to access the Ethernet submenu.

```

=====<File CONTROL>=====
|Note:the operating device is cfa0|
|<1> Download Image Program To SDRAM And Run|
|<2> Update Main Image File|
|<3> Update Backup Image File|
|<4> Download Files(*.*)|
|<5> Modify Ethernet Parameter|
|<0> Exit To Main Menu|
=====
Enter your choice(0-4):

```

Table 26 Ethernet submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download a system software image to the SDRAM and run the image.
<2> Update Main Image File	Upgrade the main system software image.

<3> Update Backup Image File	Upgrade the backup system software image.
<4> Download Files(*.*)	Download a system software image to the Cfa0 or CF card.
<5> Modify Ethernet Parameter	Modify network settings.
<0> Exit To Main Menu	Return to the BootWare menu.

2. Enter 5 to configure the network settings.

```

=====<ETHERNET PARAMETER SET>=====
|Note:      '.' = Clear field.                |
|           '-' = Go to previous field.        |
|           Ctrl+D = Quit.                    |
=====

Protocol (FTP or TFTP) :ftp
Load File Name         :msr3000.ipe
                        :
Target File Name       :msr3000.ipe
                        :
Server IP Address      :192.168.1.1
Local IP Address       :192.168.1.100
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
FTP User Name          :user001
FTP User Password      :*****

```

Table 27 Network parameter fields and shortcut keys

Field	Description
'.' = Clear field	Press a dot (.) and then Enter to clear the setting for a field.
'-' = Go to previous field	Press a hyphen (-) and then Enter to return to the previous field.
Ctrl+D = Quit	Press Ctrl + D to exit the Ethernet Parameter Set menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to FTP or TFTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file on the router. By default, the target file name is the same as the source file name.
Server IP Address	Set the IP address of the FTP or TFTP server. If a mask must be set, use a colon (:) to separate the mask length from the IP address. For example, 192.168.80.10:24.
Local IP Address	Set the IP address of the router.
Subnet Mask	Subnet Mask of the local IP address.
Gateway IP Address	Set a gateway IP address if the router is on a different network than the server.
FTP User Name	Set the username for accessing the FTP server. This username must be the same as configured on the FTP server. This field is not available for TFTP.
FTP User Password	Set the password for accessing the FTP server. This password must be the same as configured on the FTP server. This field is not available for TFTP.

3. Select an option in the Ethernet submenu to upgrade a system software image. For example, enter 2 to upgrade the main system software image.

```
Loading.....
.....
.....Done.
37691392 bytes downloaded!
The file is exist,will you overwrite it? [Y/N]Y
Image file msr3000-cmw710-boot-r6749P14.bin is self-decompressing...
Saving file cfa0:/msr3000-cmw710-boot-r6749P14.bin .....
.....Done.
Image file msr3000-cmw710-system-r6749P14.bin is self-decompressing...
Saving file cfa0:/msr3000-cmw710-system-r6749P14.bin .....
.....Done.
Image file msr3000-cmw710-security-r6749P14.bin is self-decompressing...
Saving file cfa0:/msr3000-cmw710-security-r6749P14.bin Done.
Image file msr3000-cmw710-voice-r6749P14.bin is self-decompressing...
Saving file cfa0:/msr3000-cmw710-voice-r6749P14.bin .....Done.
Image file msr3000-cmw710-data-r6749P14.bin is self-decompressing...
Saving file cfa0:/msr3000-cmw710-data-r6749P14.bin ..Done.
```

```
=====<Enter Ethernet SubMenu>=====
|Note:the operating device is cfa0                                     |
|<1> Download Image Program To SDRAM And Run                         |
|<2> Update Main Image File                                          |
|<3> Update Backup Image File                                       |
|<4> Download Files(*.*)                                           |
|<5> Modify Ethernet Parameter                                      |
|<0> Exit To Main Menu                                             |
|<Ensure The Parameter Be Modified Before Downloading!>           |
=====
Enter your choice(0-4):
```

4. Enter 0 to return to the BootWare menu

```
=====<EXTEND-BOOTWARE MENU>=====
|<1> Boot System                                                    |
|<2> Enter Serial SubMenu                                          |
|<3> Enter Ethernet SubMenu                                       |
|<4> File Control                                                  |
|<5> Modify BootWare Password                                      |
|<6> Skip Current System Configuration                             |
|<7> BootWare Operation Menu                                       |
|<8> Skip authentication for console login                         |
|<9> Storage Device Operation                                     |
|<0> Reboot                                                        |
=====
Enter your choice(0-9):
```

5. 1 to boot the system.

```

Loading the main image files...
Loading file cfa0:/msr3000-cmw710-system-r6749P14.bin.....
Done.
Loading file cfa0:/msr3000-cmw710-boot-r6749P14.bin.....Done.

Image file cfa0:/msr3000-cmw710-boot-r6749P14.bin is self-decompressing.....
.....Done.
System image is starting...
Line aux0 is available.

Press ENTER to get started.

```

Using XMODEM to upgrade software through the console port

1. Enter 2 in the BootWare menu to access the Serial submenu.

```

=====<Enter Serial SubMenu>=====
|Note:the operating device is cfa0                                     |
|<1> Download Image Program To SDRAM And Run                         |
|<2> Update Main Image File                                          |
|<3> Update Backup Image File                                       |
|<4> Download Files(*.*)                                            |
|<5> Modify Serial Interface Parameter                              |
|<0> Exit To Main Menu                                              |
=====
Enter your choice(0-4):

```

Table 28 Serial submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download an application to SDRAM through the serial port and run the program.
<2> Update Main Image File	Upgrade the main system software image.
<3> Update Backup Image File	Upgrade the backup system software image.
<4>Download Files(*.*)	Download a system software image to the Cfa0 or CF card.
<5> Modify Serial Interface Parameter	Modify serial port parameters
<0> Exit To Main Menu	Return to the BootWare menu.

2. Select an appropriate baud rate for the console port. For example, enter 5 to select 115200 bps.

```

=====<BAUDRATE SET>=====
|Note:'*'indicates the current baudrate                             |
|    Change The HyperTerminal's Baudrate Accordingly                |
|-----<Baudrate Available>-----|
|<1> 9600(Default)*                                                |
|<2> 19200                                                           |
|<3> 38400                                                           |

```

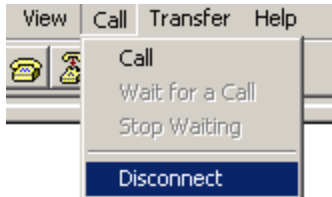
```
|<4> 57600 |
|<5> 115200 |
|<0> Exit |
=====
Enter your choice(0-5):
The following messages appear:
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

NOTE:

Typically the size of a .bin file is over 10 MB. Even at 115200 bps, the download takes about 30 minutes.

3. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the router.

Figure 2 Disconnect the terminal connection

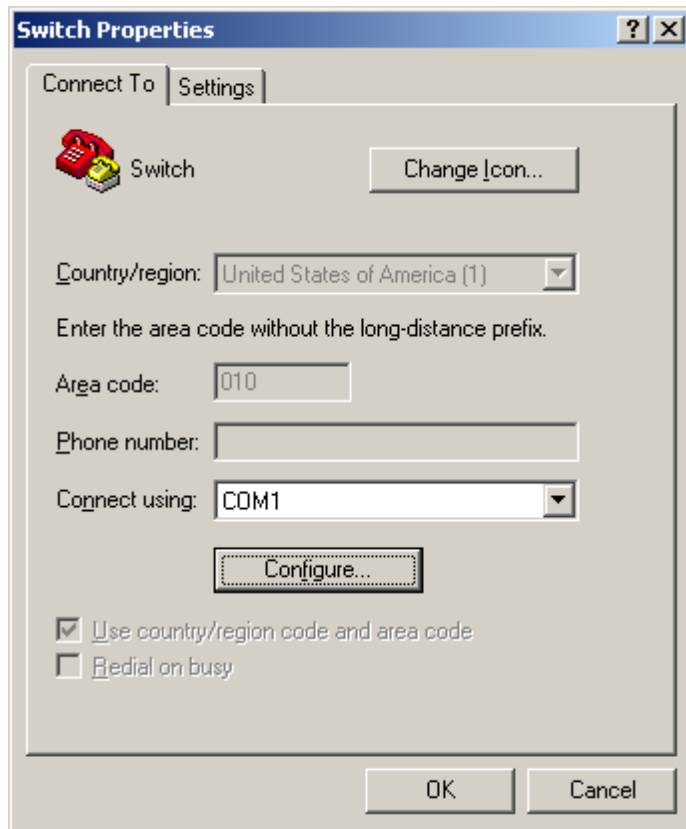


NOTE:

If the baud rate of the console port is 9600 bps, jump to step 9.

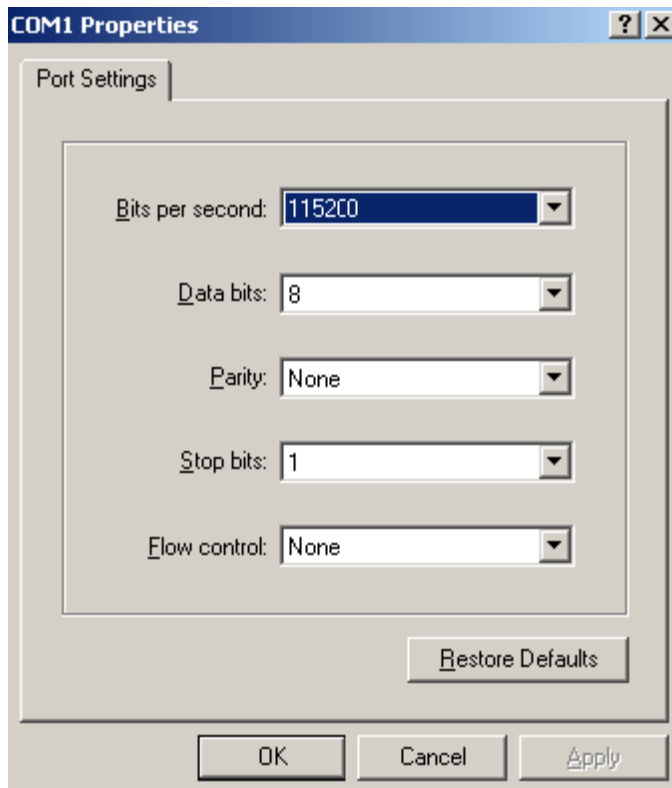
4. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



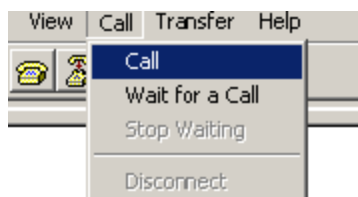
5. Select **115200** from the **Bits per second** list and click **OK**.

Figure 4 Modify the baud rate



6. Select **Call > Call** to reestablish the connection.

Figure 5 Reestablish the connection



7. Press **Enter**.

The following menu appears:

The current baudrate is 115200 bps

```
=====<BAUDRATE SET>=====
|Note:'' indicates the current baudrate                               |
|    Change The HyperTerminal's Baudrate Accordingly                 |
|-----<Baudrate Available>-----|
|<1> 9600(Default)                                                    |
|<2> 19200                                                            |
|<3> 38400                                                            |
|<4> 57600                                                            |
|<5> 115200*                                                         |
|<0> Exit                                                            |
=====
Enter your choice(0-5):
```

8. Enter **0** to return to the Serial submenu.

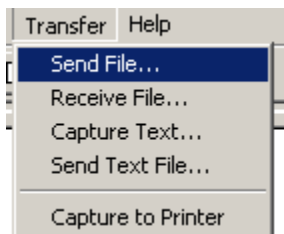
```
=====<Enter Serial SubMenu>=====
|Note:the operating device is cfa0      |
|<1> Download Image Program To SDRAM And Run      |
|<2> Update Main Image File                  |
|<3> Update Backup Image File                |
|<4> Download Files(*.*)                    |
|<5> Modify Serial Interface Parameter        |
|<0> Exit To Main Menu                      |
=====
Enter your choice(0-4):
```

9. Select an option from options **2** to **3** to upgrade a system software image. For example, enter **2** to upgrade the main system software image.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

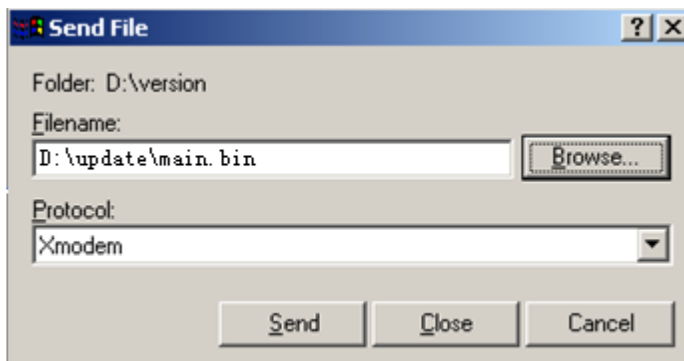
10. Select **Transfer > Send File** in the HyperTerminal window.

Figure 6 Transfer menu



11. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 File transmission dialog box



12. Click **Send**. The following dialog box appears:

Figure 8 File transfer progress

13. When the Serial submenu appears after the file transfer is complete, enter **0** at the prompt to return to the BootWare menu.

```
Download successfully!
37691392 bytes downloaded!
Input the File Name:main.bin
Updating File cfa0:/main.bin.....
.....Done!

=====<Enter Serial SubMenu>=====
|Note:the operating device is cfa0                                     |
|<1> Download Image Program To SDRAM And Run                          |
|<2> Update Main Image File                                           |
|<3> Update Backup Image File                                         |
|<4> Download Files(*.*)                                              |
|<5> Modify Serial Interface Parameter                                |
|<0> Exit To Main Menu                                                |
=====
Enter your choice(0-4):
```

14. Enter **1** in the BootWare menu to boot the system.
15. If you are using a download rate other than 9600 bps, change the baud rate of the terminal to 9600 bps. If the baud rate has been set to 9600 bps, skip this step.

Managing files from the BootWare menu

To change the type of a system software image, retrieve files, or delete files, enter **4** in the BootWare menu.

The File Control submenu appears:

```
=====<File CONTROL>=====
|Note:the operating device is cfa0                                     |
```

```

|<1> Display All File(s) |
|<2> Set Image File type |
|<3> Set Bin File type |
|<4> Set Configuration File type |
|<5> Delete File |
|<6> Copy File |
|<0> Exit To Main Menu |
=====
Enter your choice(0-6):

```

Table 29 File Control submenu options

Item	Description
<1> Display All File	Display all files.
<2> Set Image File type	Change the type of a system software image (.ipe).
<3> Set Bin File type	Change the type of a system software image (.bin).
<4> Set Configuration File type	Change the type of a configuration file.
<5> Delete File	Delete files.
<6> Copy File	Copy File
<0> Exit To Main Menu	Return to the BootWare menu.

Displaying all files

To display all files, enter **1** in the File Control submenu:

Display all file(s) in cfa0:

'M' = MAIN 'B' = BACKUP 'N/A' = NOT ASSIGNED

```

=====
|NO. Size(B)   Time                Type   Name                                     |
|1   37691392  Aug/16/2020 07:09:16 N/A    cfa0:/msr3000.ipe                     |
|2   25992     Aug/15/2020 12:18:00 N/A    cfa0:/startup.mdb                     |
|3   1632      Aug/15/2020 12:18:00 M      cfa0:/startup.cfg                     |
|4   84        Aug/15/2020 12:17:59 N/A    cfa0:/ifindex.dat                     |
|5   11029     Aug/15/2020 13:31:16 N/A    cfa0:/logfile/logfile1.log            |
|6   17        Aug/16/2020 07:47:24 N/A    cfa0:/pathfile                         |
|7   1006592   Aug/16/2020 07:44:16 M      cfa0:/msr3000-cmw710-data-r6749P14.bin|
|8   815       Aug/15/2020 12:03:14 N/A    cfa0:/license/DeviceID.did            |
|9   1180672   Aug/16/2020 07:44:15 M      cfa0:/msr3000-cmw710-voice-r6749P14. bin|
|10  10240     Aug/16/2020 07:44:15 M      cfa0:/msr3000-cmw710-security-r6749P14.bin|
|11  24067072  Aug/16/2020 07:44:10 M      cfa0:/msr3000-cmw710-system-r6749P14.bin|
|12  11418624  Aug/16/2020 07:44:05 M      cfa0:/msr3000-cmw710-boot-r6749P14.bin|
=====

```

Changing the type of a system software image

System software image file attributes include main (M), and backup (B). You can store only one main image, and one backup image on the router. A system software image can have any combination of the M, and B attributes. If the file attribute you are assigning has been assigned to an image, the

assignment removes the attribute from that image. The image is marked as N/A if it has only that attribute.

To change the type of a system software image:

1. Enter **2** in the File Control submenu.

```
'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED

=====
|NO. Size(B)   Time                Type   Name                               |
|1   37691392  Aug/16/2020 07:09:16 N/A    cfa0:/msr3000.ipe                 |
|0   Exit                                           |
=====

Enter file No:1
```

2. Enter the number of the file you are working with, and press **Enter**.

```
Modify the file attribute:

=====
|<1> +Main                                           |
|<2> +Backup                                          |
|<0> Exit                                           |
=====

Enter your choice(0-2):
```

3. Enter a number in the range of 1 to 4 to add or delete a file attribute for the file.

Set the file attribute success!

Deleting files

When storage space is insufficient, you can delete obsolete files to free up storage space.

To delete files:

1. Enter **5** in the File Control submenu.

```
Deleting the file in cfa0:
'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED

Deleting the file in cfa0:
'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED

=====
|NO. Size(B)   Time                Type   Name                               |
|1   37691392  Aug/16/2020 07:09:16 N/A    cfa0:/msr3000.ipe                 |
|2   25992     Aug/15/2020 12:18:00 N/A    cfa0:/startup.mdb                 |
|3   1632      Aug/15/2020 12:18:00 M      cfa0:/startup.cfg                 |
|4   84        Aug/15/2020 12:17:59 N/A    cfa0:/ifindex.dat                 |
|5   11029     Aug/15/2020 13:31:16 N/A    cfa0:/logfile/logfile1.log        |
|6   17        Aug/16/2020 07:47:24 N/A    cfa0:/pathfile                    |
|7   1006592   Aug/16/2020 07:44:16 M      cfa0:/msr3000-cmw710-data-r6749P14.bin|
|8   815       Aug/15/2020 12:03:14 N/A    cfa0:/license/DeviceID.did        |
|9   1180672   Aug/16/2020 07:44:15 M      cfa0:/msr3000-cmw710-voice-r6749P14.bin|
|10  10240     Aug/16/2020 07:44:15 M      cfa0:/msr3000-cmw710-security-r6749P14.bin|
|11  24067072  Aug/16/2020 07:44:10 M      cfa0:/msr3000-cmw710-system-r6749P14.bin|
|12  11418624  Aug/16/2020 07:44:05 M      cfa0:/msr3000-cmw710-boot-r6749P14.bin|
|0   Exit                                           |
=====

Enter file No.:
```

2. Enter the number of the file to delete.

3. When the following prompt appears, enter Y.

```
The file you selected is cfa0:/msr3000-cmw710-security-r6749P14.bin,Delete it?  
[Y/N]Y  
Deleting...Done.
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version. To handle a software failure:

1. Check the physical ports for a loose or incorrect connection.
2. If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.
3. Check the file transfer settings:
 - If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
 - If TFTP is used, you must enter the same server IP addresses, file name, and working directory as set on the TFTP server.
 - If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as set on the FTP server.
4. Check the FTP or TFTP server for any incorrect setting.
5. Check that the storage device has sufficient space for the upgrade file.
6. If the message “Something is wrong with the file” appears, check the file for file corruption.

Appendix C Handling console login password loss

Disabling password recovery capability

Password recovery capability controls console user access to the device configuration and SDRAM from BootWare menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security, disable password recovery capability.

[Table 30](#) summarizes options whose availability varies with the password recovery capability setting.

Table 30 BootWare options and password recovery capability compatibility matrix

BootWare menu option	Password recovery enabled	Password recovery disabled	Tasks that can be performed
Download Image Program To SDRAM And Run	Yes	No	Load and run Comware software images in SDRAM.

Skip Authentication for Console Login	Yes	No	Enable console login without authentication.
Skip Current System Configuration	Yes	No	Load the factory-default configuration without deleting the next-startup configuration files.
Restore to Factory Default Configuration	No	Yes	Delete the next-startup configuration files and load the factory-default configuration.

To disable password recovery capability:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable password recovery capability.	undo password-recovery enable	By default, password recovery capability is enabled.

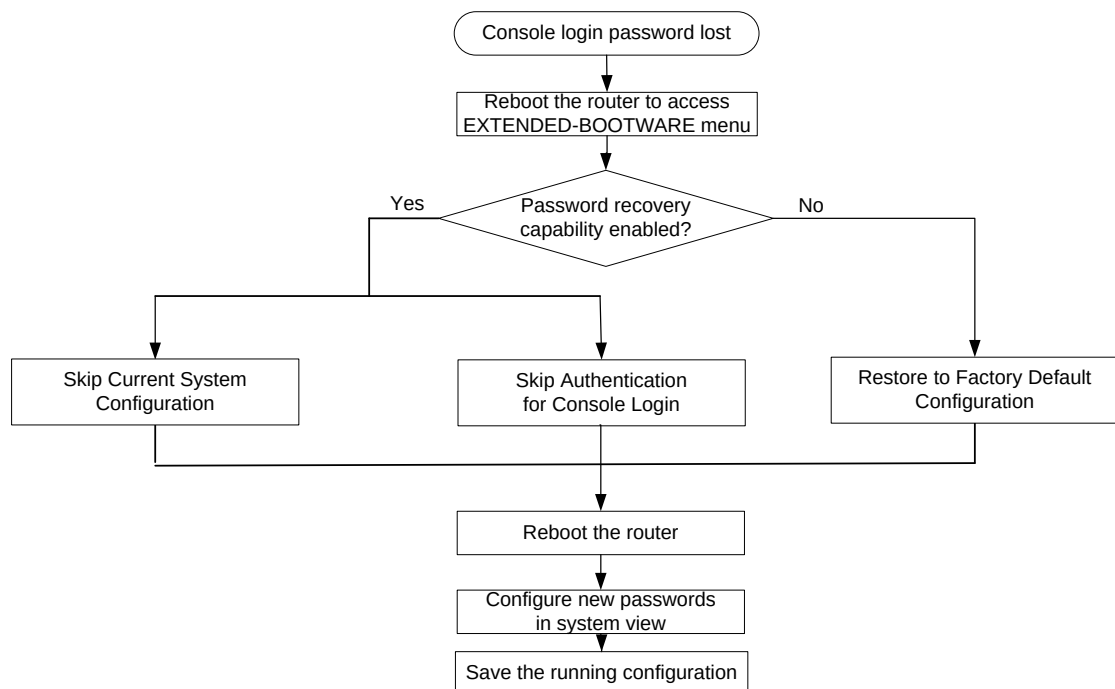
When password recovery capability is disabled, you cannot downgrade the device software to a version that does not support the capability through the BootWare menus. You can do so at the CLI, but the BootWare menu password configured becomes effective again.

Handling console login password loss

CAUTION:
Handling console login password loss causes service outage.

The method for handling console login password loss depends on the password recovery capability setting (see [Figure 9](#)).

Figure 9 Handling console login password loss



Examining the password recovery capability setting

1. Reboot the router.

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start heavy memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing....Done.

*****
*
*                               HPE MSR3012 BootWare, Version 1.82
*
*****
Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP

Compiled Date      : Jul 14 2020
CPU ID            : 0x2
Memory Type       : DDR3 SDRAM
Memory Size       : 1024MB
Flash Size        : 8MB
cfa0 Size         : 247MB
CPLD Version      : 2.0
PCB Version       : 2.0
```

```
BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
```

2. Press **Ctrl + B** within three seconds after the "Press Ctrl+B to access EXTENDED-BOOTWARE MENU..." prompt message appears.
3. Read the password recovery capability setting information displayed before the EXTEND-BOOTWARE menu.

```
Password recovery capability is enabled.
```

```
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.
```

```
=====<EXTEND-BOOTWARE MENU>=====
|<1> Boot System                               |
|<2> Enter Serial SubMenu                     |
|<3> Enter Ethernet SubMenu                   |
|<4> File Control                             |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration        |
|<7> BootWare Operation Menu                  |
|<8> Skip Authentication for Console Login    |
|<9> Storage Device Operation                 |
|<0> Reboot                                  |
=====
```

```
Ctrl+Z: Access EXTEND ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9):
```

Using the Skip Current System Configuration option

1. Reboot the router to access the EXTEND-BOOTWARE menu, and then enter 6.

The current mode is password recovery.

Note: The current operating device is cfa0

Enter < Storage Device Operation > to select device.

```
=====<EXTEND-BOOTWARE MENU>=====
|<1> Boot System                                     |
|<2> Enter Serial SubMenu                           |
|<3> Enter Ethernet SubMenu                         |
|<4> File Control                                   |
|<5> Restore to Factory Default Configuration       |
|<6> Skip Current System Configuration               |
|<7> BootWare Operation Menu                       |
|<8> Skip Authentication for Console Login          |
|<9> Storage Device Operation                       |
|<0> Reboot                                         |
=====
Ctrl+Z: Access EXTEND ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 6
```

After the configuration skipping flag is set successfully, the following message appears:

Flag Set Success.

2. When the EXTEND-BOOTWARE menu appears again, enter 1 to reboot the router.
The router starts up with the factory-default configuration without deleting the next-startup configuration files.
3. To use the configuration in a next-startup configuration file, load the file in system view.

```
<HPE> system-view
[HPE] configuration replace file cfa0:/startup.cfg
Current configuration will be lost, save current configuration? [Y/N]:n
Info: Now replacing the current configuration. Please wait...
Info: Succeeded in replacing current configuration with the file startup.cfg.
```

4. Configure a new console login authentication mode and a new console login password.

In the following example, the console login authentication mode is password and the authentication password is 123456. For security purposes, the password is always saved in ciphertext, whether you specify the **simple** or **cipher** keyword for the **set authentication password** command.

```
<HPE> system-view
[HPE] line aux 0
[HPE-line-aux0] authentication-mode password
[HPE-line-aux0] set authentication password simple 123456
```

Use the **line aux 0** command on an MSR2000 or MSR 3000 routers. The console port and the AUX port are the same physical port.

Use the **line console 0** command on an MSR4000 routers. An MSR4000 router has a separate console port.

5. To make the settings take effect after a reboot, save the running configuration to the next-startup configuration file.

```
[HPE-line-aux0] save
```

Using the Skip Authentication for Console Login option

1. Reboot the router to access the EXTEND-BOOTWARE menu, and then enter 8.

The current mode is password recovery.

Note: The current operating device is cfa0

Enter < Storage Device Operation > to select device.

```
=====<EXTEND-BOOTWARE MENU>=====
```

```
|<1> Boot System |
|<2> Enter Serial SubMenu |
|<3> Enter Ethernet SubMenu |
|<4> File Control |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration |
|<7> BootWare Operation Menu |
|<8> Skip Authentication for Console Login |
|<9> Storage Device Operation |
|<0> Reboot |
```

```
=====
Ctrl+Z: Access EXTEND ASSISTANT MENU
```

```
Ctrl+F: Format File System
```

```
Enter your choice(0-9): 8
```

The router deletes the console login authentication configuration commands from the main next-startup configuration file. After the operation is completed, the following message appears:

```
Clear Image Password Success!
```

2. When the EXTEND-BOOTWARE menu appears again, enter 1 to reboot the router.
The router starts up with the main next-startup configuration file.
3. Configure a console login authentication mode and a new console login password. See "Configure a new console login authentication mode and a new console login password.Configure a new console login authentication mode and a new console login password."
4. To make the setting take effect after a reboot, save the running configuration to the next-startup configuration file.

```
[HPE-line-aux0] save
```

Using the Restore to Factory Default Configuration option

CAUTION:

Using the Restore to Factory Default Configuration option deletes both the main and backup next-configuration files.

1. Reboot the router to access the EXTEND-BOOTWARE menu, and enter 5.

The current mode is no password recovery.

Note: The current operating device is cfa0

Enter < Storage Device Operation > to select device.

```
=====<EXTEND-BOOTWARE MENU>=====
```

```
|<1> Boot System |
|<2> Enter Serial SubMenu |
|<3> Enter Ethernet SubMenu |
|<4> File Control |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration |
|<7> BootWare Operation Menu |
|<8> Skip Authentication for Console Login |
|<9> Storage Device Operation |
|<0> Reboot |
```

```
=====
```

Ctrl+Z: Access EXTEND ASSISTANT MENU

Ctrl+F: Format File System

Enter your choice(0-9): 5

2. At the prompt for confirmation, enter Y.

The router deletes its main and backup next-startup configuration files and restores the factory-default configuration.

The current mode is no password recovery. The configuration files will be deleted, and the system will start up with factory defaults, Are you sure to continue?[Y/N]Y

Setting...Done.

3. When the EXTEND-BOOTWARE menu appears again, enter 1 to reboot the router.

The router starts up with the factory-default configuration.

4. Configure a new console login authentication mode and a new console login password. See "Configure a new console login authentication mode and a new console login password.Configure a new console login authentication mode and a new console login password."

5. To make the settings take effect after a reboot, save the running configuration to the next-startup configuration file.

[HPE] save



Hewlett Packard
Enterprise

HPE MSR1000_MSR2000_MSR3000_MSR4000_ MSR9XX-CMW710-R6728P25 Release Notes Software Feature Changes

The information in this document is subject to change without notice.
© Copyright 2013, 2022 Hewlett Packard Enterprise Development LP

Contents

Release 6749P14.....	52
New feature: Link flapping protection on an interface	57
Enabling link flapping protection on an interface.....	57
Command reference	58
New command: display link-flap protection	58
New command: display link-state-change statistics interface	59
New command: link-flap protect enable	60
New command: port link-flap protect enable	61
New command: reset link-state-change statistics interface	62
New feature: SRv6 and MPLS interworking.....	63
Configuring SRv6 and MPLS interworking	63
Configuring inter-AS option B VPN	63
Configuring optimal route reorigination and advertisement	64
SRv6 and MPLS interworking	65
srv6-mpls-interworking enable	65
advertise route-reoriginate	66
Modified command: segment-routing ipv6 best-effort	67
Modified command: segment-routing ipv6 locator	68
Modified command: segment-routing ipv6 traffic-engineering	69
New feature: Applying a QoS policy to an SRv6 TE policy.....	70
Applying the QoS policy to an SRv6 TE policy	70
Command reference	70
qos apply policy srv6-policy	70
reset qos policy srv6-policy	71
display qos policy srv6-policy.....	72
New feature: SRv6 service chain	73
Creating an SRv6 service chain	73
Creating an SRv6 service chain in static proxy mode	73
Creating an SRv6 service chain in masquerading mode	74
Configuring the encapsulation method for packets between a pair of SFF and SF	75
Configuring the packet encapsulation method for an SRv6 service chain in static proxy mode	75
Configuring the packet encapsulation method for an SRv6 service chain in masquerading mode	76
Configuring packet reencapsulation parameters for an SRv6 service chain in static proxy mode	77
Configuring the DiffServ mode for an SRv6 service chain in static proxy mode	78
Configuring the TTL mode for an SRv6 service chain in static proxy mode.....	79
Configuring dualhoming protection for an SRv6 service chain in static proxy mode	80
Configuring bypass protection for an SRv6 service chain in static proxy mode	80
Using static BFD in echo packet mode to detect SF reachability.....	81
Command reference	82
New command: backup-opcode	82
New command: bypass	83
New command: cache list	84
New command: cache source-address	85
New command: display segment-routing ipv6 sfc forwarding	86
New command: encapsulation eth out-interface	87
New command: encapsulation ipv4 nexthop	90
New command: encapsulation ipv6 nexthop	92
New command: inner-type	94
New command: opcode end-am	95
New command: opcode end-as	96
New command: proxy peer-sid	97
New command: sfc diffserv-mode	97

New command: sfc ttl-mode	99
Modified command: display segment-routing ipv6 local-sid	99
New feature: Configuring 8-queue PQ	100
Configuring 8-queue PQ	100
Command reference	101
Modified command: qos pql default-queue	101
Modified command: qos pql inbound-interface	101
Modified command: qos pql local-precedence	102
Modified command: qos pql protocol	102
Modified command: qos pql protocol mpls exp	103
Modified command: qos pql queue	103
New feature: Configuring an SDWAN TTE information match criterion and a VPN instance match criterion	104
Configuring an SDWAN TTE information match criterion and a VPN instance match criterion	104
Command reference	105
Modified command: if-match	105
New feature: Simplifying the QoS configuration in a hub-spoke network	105
Simplifying the QoS configuration in a hub-spoke network	105
Command reference	107
New command: display qos policy sdwan	107
New command: qos apply user-profile downstream	108
New command: reset qos policy sdwan	109
Modified command: display qos tunnel-session	110
Modified command: reset qos tunnel-session	111
New command: qos lr outbound (user profile view)	111
New command: qos bandwidth downstream	112
New command: qos pq (user profile view)	113
New feature: Configuring interface channelization	114
Configuring interface channelization	114
Command reference	114
New command: display mode channel-bandwidth interface	114
New command: mode channel-bandwidth	116
New feature: Configuring a default color value for public network and L3VPN route recursion to an SRv6 TE policy	117
Configure a default color value for public network and VPN route recursion to an SRv6 TE policy	117
Command reference	118
default-color (public instance IPv4/IPv6 address family view)	118
default-color (VPN instance IPv4/IPv6 address family view)	119
New feature: SRv6 TE policy route recursion support for SRv6-TE and SRv6-BE FRR mode	120
Configuring SRv6-TE and SRv6-BE FRR mode	120
Command reference	121
Modified command: segment-routing ipv6 traffic-engineering	121
New feature: Configuring the SRv6 TE policy encapsulation mode	122
Configuring the SRv6 TE policy encapsulation mode	122
Command reference	124
New command: encapsulation-mode	124
New command: encapsulation-mode encaps include local-end.x	126
New command: encapsulation-mode insert include local-end.x	127
New command: srv6-policy encapsulation-mode	128
New command: srv6-policy encapsulation-mode encaps include local-end.x	129
New command: srv6-policy encapsulation-mode insert include local-end.x	130
Modified command: display segment-routing ipv6 local-sid	131

New feature: Configuring the Next Header field value in the SRH of SRv6 packets	132
Configuring the Next Header field value in the SRH of SRv6 packets	132
Command reference	132
evpn next-header-field	132
New feature: SRv6 TE policy rate limit	133
Configuring a rate limit for an SRv6 TE policy	133
Command reference	134
rate-limit	134
New feature: Configuring next hop-based dynamic End.DX4 or End.DX6 SID allocation for public or private network routes	135
Configuring next hop-based dynamic End.DX4 or End.DX6 SID allocation for public or private network routes	135
Command reference	136
nexthop interface (BGP-VPN IPv4 SR next hop view/BGP-VPN IPv4 EVPN SR next hop view)	136
nexthop interface (BGP SRv6 next hop view/BGP-VPN SRv6 next hop view/BGP-VPN IPv6 EVPN SR next hop view)	138
segment-routing ipv6 apply-sid all-nexthop (BGP IPv4/BGP IPv6 address family view)	139
segment-routing ipv6 apply-sid specify-nexthop (BGP IPv4/BGP IPv6 address family view)	140
segment-routing ipv6 apply-sid specify-nexthop (BGP-VPN IPv4/IPv6 address family view)	141
New feature: VPNv4/VPNv6/EVPN routes	143
Modifying BGP VPNv4 or VPNv6 routes	143
Command reference	144
peer re-originated	144
peer suppress re-originated	146
New feature: G-SRv6	147
Configuring G-SIDs	147
Command reference	149
New command: srv6 compress enable (IS-IS IPv6 address family view)	149
New command: srv6 compress enable (Segment Routing IPv6 view)	149
Modified command: locator	150
Modified command: opcode	151
New feature: Configuring the SRv6 MTU	153
Configuring the SRv6 MTU	153
Command reference	153
New command: path-mtu reserved	153
New feature: Configuring the SRv6 DiffServ mode	154
Configuring the SRv6 DiffServ mode	154
Command reference	155
New command: diffserv-mode	155
New feature: BGP-EPE	157
Configuring BGP EPE	157
Configuring SID allocation through BGP EPE	157
Configuring a BGP EPE peer set	158
Command reference	158
New command: egress-engineering peer-set	158
New command: peer peer-set	159
New command: display bgp egress-engineering peer-set	160
Modified command: peer egress-engineering	162
Modified command: display bgp egress-engineering ipv4	162
New feature: SRv6 TE Policy CBTS	163
Configuring SRv6 TE policy CBTS	163

Command reference	163
service-class	163
New feature: Enabling the device to distribute SRv6 TE policy candidate path information to BGP-LS	164
Enabling the device to distribute SRv6 TE policy candidate path information to BGP-LS	164
Command reference	165
distribute bgp-ls	165
New feature: SRv6 TE policy egress protection	166
Configuring SRv6 TE policy egress protection	166
Restrictions and guidelines for SRv6 TE policy egress protection configuration	166
Configuring an End.M SID	166
Enabling egress protection	166
Configuring the deletion delay time for remote SRv6 SID mappings with VPN instances/cross-connects/VSI	167
Command reference	168
fast-reroute mirror delete-delay	168
fast-reroute mirror enable	169
mirror remote-sid delete-delay	169
display bgp mirror remote-sid	170
New feature: Enabling the device to drop traffic when an SRv6 TE policy becomes invalid	171
Enabling the device to drop traffic when an SRv6 TE policy becomes invalid	171
Command reference	172
drop-upon-invalid enable	172
New feature: Automatic route advertisement for an SRv6 TE policy	173
Enabling automatic route advertisement for an SRv6 TE policy	173
Command reference	174
autoroute enable	174
autoroute metric	175
srv6-policy autoroute enable	176
New feature: EVPN VPLS over SRv6/EVPN VPWS over SRv6	177
Configuring EVPN VPLS over SRv6	177
Configuring an EVPN instance	177
Configuring SRv6 SIDs	178
Applying a locator to a VSI	178
Configuring unicast traffic forwarding based on End.DX2 and End.DX2L SIDs	179
Configuring the route recursion mode	179
Configuring color-based traffic steering	180
Configuring PEs to exchange BGP EVPN routes	181
Configuring SRv6 PW packet statistics	182
Using ping to test the connectivity of an SRv6 PW	182
Using tracer to test the connectivity of an SRv6 PW	182
Configuring EVPN VPWS over SRv6	183
Configuring a cross-connect group and its EVPN instance	183
Configuring SRv6 SIDs	184
Applying a locator to a cross-connect	185
Configuring the route recursion mode	185
Configuring color-based traffic steering	186
Configuring tunnel policy-based traffic steering	187
Configuring PEs to exchange BGP EVPN routes	188
Configuring LDP PWs as ACs for SRv6 PWs	189
Configuring static PWs as ACs for SRv6 PWs	190
Configuring SRv6 PW packet statistics	191
Using ping to test the connectivity of an SRv6 PW	191
Using tracer to test the connectivity of an SRv6 PW	192
Command reference	193

display l2vpn statistics srv6-pw inbound	193
display l2vpn xconnect-group	194
evpn encapsulation srv6	197
export route-policy	197
import route-policy	198
ping evpn vpls srv6	199
ping evpn vpws srv6	201
reset l2vpn statistics srv6-pw	203
segment-routing ipv6	203
segment-routing ipv6 locator (cross-connect view and VSI EVPN instance view)	205
statistics enable	206
tracert evpn vpls srv6	207
tracert evpn vpws srv6	209
unicast-forwarding dx2-based	210
New feature: Configuring IPv6 Flowspec	211
Configuring IPv6 Flowspec	211
Creating and activating an IPv6 Flowspec rule	211
Applying an IPv6 Flowspec rule	212
Enabling BGP to distribute IPv6 Flowspec rules	213
Configuring BGP Flowspec route reflection	215
Disabling the actions in IPv6 Flowspec rules	216
Command reference	216
New command: address-family ipv6	216
New command: address-family ipv6 flowspec (BGP instance view)	217
New command: address-family ipv6 flowspec (BGP-VPN instance view)	217
New command: address-family vpnv6 flowspec	218
Modified command: apply	219
Modified command: check flow-route-configuration	220
Modified command: commit	220
New command: display bgp group flowspec	220
New command: display bgp routing-table ipv6 flowspec	222
New command: display bgp routing-table vpnv6 flowspec	227
Modified command: display flow-route	233
Modified command: flow-route (Flowspec IPv4 address family view)	233
New command: flow-route ipv6 (system view)	234
Modified command: if-match	234
Modified command: peer next-hop-invariable	235
New command: peer redirect ip rfc-compatible	236
Modified command: peer reflect-client	237
Modified command: peer validation-disable	238
Modified command: peer validation-redirect-disable	238
Modified command: policy vpn-target	239
New command: redirect ip recursive-lookup tunnel	239
Modified command: reflect between-clients	240
Modified command: reflector cluster-id	241
Modified command: reset flow-route statistics	241
Modified command: vpn-target	241
New feature: MP packet fast forwarding	242
Configuring MP packet fast forwarding	242
Command reference	242
New command: ppp mp fast-forward enable	242
New feature: Setting the traffic statistics update timer for IPoE sessions	243
Setting the traffic statistics update timer for IPoE sessions	243
Command reference	243
New command: ip subscriber timer traffic	243
New command: ipv6 subscriber timer traffic	244

New feature: Configuring the time interval for traffic rate calculation of portal users	245
Configuring the time interval for traffic rate calculation of portal users	245
Command reference	245
New command: portal traffic-rate statistics-interval	245
Modified command: display portal user	246
New feature: Disabling sending a specific type of ICMP messages	246
Disabling sending a specific type of ICMP messages	246
Command reference	247
ip icmp send enable	247
New feature: Disabling receiving a specific type of ICMP messages	249
Disabling receiving a specific type of ICMP messages	249
Command reference	249
ip icmp receive enable	249
New feature: Display the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state	251
Displaying the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state	251
Command reference	251
display link-aggregation troubleshooting	251
New feature: Python2 progress monitoring	254
Feature description	254
New feature	254
New feature: Software upgrade through CWMP	254
Software upgrade through CWMP	254
New feature: Specifying a CPE service port number	255
Specifying a CPE service port number	255
Command reference	256
cwmp cpe port	256
New feature: Configuring the notification format and enabling notifications to carry the device serial number (SN)	256
Configuring the notification format and enabling notifications to carry the device serial number	256
Command reference	257
snmp-agent trap format	257
snmp-agent trap withsn	257
New feature: Configuring SQA	258
About this task	258
Restrictions: Hardware compatibility with SQA	258
Restrictions and guidelines: SQA configuration	260
Configuring SIP-based SQA	260
Configuring H.323-based SQA	260
Display and maintenance commands for SQA	260
Command reference	261
display sqa call	261
display sqa call-statistics	264
sqa	265
sqa-h323 enable	265
sqa-sip enable	266

New feature: Specifying the number of CPU cores allocated as control cores	267
Specifying the number of CPU cores as control cores	267
Command reference	269
allocate core	269
display core allocation	272
New feature: Enabling the capability of MPLS BFD to trigger tunnel-down	274
Enable the capability of MPLS BFD to trigger tunnel-down	274
Command reference	275
mpls bfd trigger tunnel-down	275
mpls bfd trigger tunnel-down enable	276
New feature: Configuring resource monitoring	277
Configuring resource monitoring	277
Command reference	280
display resource-monitor	280
resource-monitor minor resend enable	283
resource-monitor output	284
resource-monitor resource	285
New feature: Tunnel BFD for LSPs	288
Configuring tunnel BFD for LSPs	288
Command reference	290
mpls tunnel-bfd (for LSP)	290
New feature: Tunnel BFD for MPLSTE tunnels	292
Configuring tunnel BFD for MPLS TE tunnels	292
Command reference	294
mpls tunnel-bfd (for TE tunnel)	294
New feature: Configuring the rule for adding BGP routes to the IP routing table and the route advertisement rule for VPN instances	295
Configuring the rule for adding BGP routes to the IP routing table and the route advertisement rule for VPN instances	296
Command reference	297
New command: bestroute same-rd	297
Modified command: display bgp routing-table vpnv4	298
Modified command: display bgp routing-table vpnv6	299
New feature: Specifying an MPLS label allocation mode	299
Specifying an MPLS label allocation mode	299
Command reference	300
New feature: Setting an MPLS label range for all VPN instances	301
Setting an MPLS label range for all VPN instances	301
Command reference	301
mpls per-vrf-label range	301
New feature: Applying the export routing policy to VPNv4 routes before RT filtering	302
Applying the export routing policy to VPNv4 routes before RT filtering	302
Command reference	302
rtfilter check-after-policy	302
New feature: Configuring a BJCA authentication server	303
Configuring a BJCA authentication server	303
Command reference	304
aaa bjca-auth-server	304

New feature: Enabling transparent transmission of LLDP frames	305
Enabling transparent transmission of LLDP frames	305
Command reference	306
lldp transparent enable	306
New feature: Transparent LACPDU transmission	306
Enabling transparent LACPDU transmission	306
Command reference	307
lacp transparent enable	307
New feature: Configuring VLAN mapping	308
Configuring VLAN mapping	308
About VLAN mapping	308
VLAN mapping types	308
VLAN mapping application scenarios	308
VLAN mapping implementations	309
Restrictions and guidelines: VLAN mapping configuration	312
VLAN mapping tasks at a glance	312
Prerequisites	312
Configuring one-to-two VLAN mapping	312
Configuring zero-to-two VLAN mapping	313
Configuring two-to-two VLAN mapping	314
VLAN mapping commands	315
display vlan mapping	315
vlan mapping	315
vlan mapping untagged	317
New feature: PKI domain for communication with a JIT authentication server	318
Specifying a PKI domain for communication with a JIT authentication server	318
pki-domain	318
New feature: SDWAN	319
About SDWAN	319
Restrictions: Licensing requirements for SDWAN	319
SDWAN network model	319
SDWAN packet formats	320
Control packet format	320
Data packet format	321
BGP extensions	322
BGP IPv4 tunnel-encap-ext address family	322
BGP EVPN routes	323
Channel establishment	323
Control channel establishment	324
Data channel establishment	324
Route advertisement	325
Traffic forwarding	327
IPsec-protected SDWAN tunnels	327
SDWAN tunnel establishment with NAT traversal	328
About this feature	328
Control channel establishment	329
Data channel establishment	330
SDWAN tasks at a glance	331
Configuring site and device identification information	332
Specifying a site for the device	332
Specifying an ID and system IPv4 address for the device	332
Configuring an SDWAN client	333
Configuring an SDWAN server	333
Configuring an SDWAN tunnel	334
Testing TTE connection connectivity	336

About testing TTE connection connectivity	336
Restrictions and guidelines for testing TTE connection connectivity	336
Using BFD to test TTE connection connectivity	336
Using keepalive to test TTE connection connectivity	337
Configuring BGP to advertise IPv4 tunnel-encap-ext routes	337
Restrictions and guidelines for BGP IPv4 tunnel-encap-ext route advertisement	337
Enabling BGP to advertise BGP IPv4 tunnel-encap-ext routes	337
Configuring BGP IPv4 tunnel-encap-ext route settings	338
Maintaining BGP sessions	339
Using BGP EVPN IP prefix advertisement routes to advertise routes for a VPN instance	340
Configuring a CPE	340
Configuring an RR	341
Configuring traffic rerouting and load balancing by using the Priority-Color attribute	342
Configuring next hop recursion based on only the Priority-Color attribute for IP prefix advertisement routes	344
Configuring SDWAN network intercommunication over an EVPN VXLAN network	345
Configuring SDWAN network intercommunication with an EVPN L3VPN over SRv6 network	347
Specifying the post-NAT public IP address and port number for tunneled packets	349
Simplifying the QoS configuration on a hub-spoke network	349
Command reference	350
address-family ipv4 tnl-encap-ext	350
display bgp routing-table ipv4 tnl-encap-ext	351
display sdwan peer-connection status	362
display sdwan server status	363
display sdwan site-tte	364
display sdwan tte connection	367
evpn-sdwan nexthop-recursive priority-color-only	368
evpn sdwan routing-enable	370
reset sdwan tte connection	370
peer advertise encap-type sdwan	371
sdwan bfd enable	372
sdwan device-id	373
sdwan encapsulation global-udp-port	373
sdwan encapsulation udp-port	374
sdwan group-id	375
sdwan interface-id	376
sdwan keepalive	376
sdwan nat-global-ip	377
sdwan routing-domain	378
sdwan server	379
sdwan server enable	380
sdwan server port	381
sdwan site-id	381
sdwan site-name	382
sdwan site-role	383
sdwan ssl-server-policy	383
sdwan ssl-client-policy	384
sdwan system-ip	385
sdwan transport-network	386
sdwan vn-id	387
New feature: STUN	387
About STUN	387
Basic concepts	387
NAT mapping and filtering	388
NAT types	391
Application scenarios	392
STUN packet structure	392
How STUN works	394
STUN server deployment in private networks	397
Client retransmissions	398
Protocols and standards	398

Restrictions and guidelines: STUN configuration	398
STUN tasks at a glance	399
Prerequisites for STUN	399
Configure the STUN server	399
Configure the STUN client	399
Command reference	400
display stun client info	400
display stun server packet-statistics	401
reset stun client statistics	402
reset stun server packet-statistics	402
stun client	403
stun server	404
New feature: Cloud connections	406
About cloud connections	406
Multiple subconnections	406
Cloud connection establishment	406
Configuring the cloud server	407
Configuring the local device	407
Unbinding the device from the cloud server	410
Command reference	410
cloud-management backup-server domain	410
cloud-management keepalive	412
cloud-management keepalive count	412
cloud-management ping	413
cloud-management server domain	414
cloud-management server password	415
cloud-management server port	416
cloud-management token	417
cloud-management unbinding-code	418
display cloud-management state	418
New feature: Specifying a CWMP NTP server	421
Configuring NTP in client/server mode	421
Command reference	422
ntp-service cwmp unicast-server	422
New feature: Enabling route advertisement for IPv6 prefixes assigned to directly connected clients	423
Enabling route advertisement for IPv6 prefixes assigned to directly connected clients	423
Command reference	424
ipv6 dhcp advertise pd-route	424
New feature: Enabling the DHCPv6 relay agent to support Option 79	425
Enabling the DHCPv6 relay agent to support Option 79	425
Command reference	425
New feature: mGRE NHS and NHRP packet sending related features	426
Configuring new features on an NHS	426
Configuring new features on an NHC	426
Command changes	427
New command: display nhrp history-map	427
New command: nhrp dscp	428
New command: nhrp registration no-unique	429
New command: nhrp registration time-out	430
New command: nhrp server-only	430
New command: reset nhrp dynamic map	431
New command: reset nhrp history-map	431
Modified command: display mgre session	432
Modified command: display nhrp map	432

New feature: Setting the length of called numbers when R2 signaling is used to access the POS terminal	433
Setting the length of called numbers when R2 signaling is used to access the POS terminal	433
Command reference	433
posa called-length	433
New feature: Establishing an MQTT connection.....	434
Establishing an MQTT connection	434
Command reference	435
display sim mqtt statistics.....	435
display sim mqtt status	438
reset sim mqtt statistics	439
sim mqtt connect.....	440
sim mqtt keepalive.....	440
sim mqtt server	441
New feature: Configuring packet duplication optimization parameters	442
Configuring packet duplication optimization parameters	442
About this task	442
Restrictions and guidelines.....	443
Enabling packet duplication RIR	443
Manually specifying a packet duplication path in an SDWAN network.....	443
Setting the packet duplication reorder timeout timer	444
Command reference	444
packet-dup reorder timeout	444
packet-dup rir enable	445
waas packet-dup sdwan static-path	446
New feature: Setting the reorder timeout timer for load balancing packets	447
Setting the reorder timeout timer for load balancing packets.....	447
Command reference	448
display waas statistics load-balance.....	448
reset waas statistics load-balance	449
waas load-balance reorder timeout	449
New feature: Configuring TCP MSS automatic adjustment	450
Configuring TCP MSS automatic adjustment	450
Command reference	453
tcp auto-adjust-mss	453
tcp auto-adjust-mss enable	454
New feature: Configuring BGP GR	455
Configuring BGP GR	455
Command reference	456
graceful-restart peer-reset.....	456
peer graceful-restart timer restart extra.....	456
New feature: Support for filtering routes by the Priority-Color extended community attribute	458
Configuring a Priority-Color extended community list	458
Command reference	458
display ip extcommunity-list.....	458
ip extcommunity-list	459
Configuring the Priority-Color extended community attribute for BGP routes.....	460
Command reference	460
apply extcommunity priority-color	460
New feature: Configuring automatic SIM registration	462
Configuring automatic SIM registration	462
Command reference	463

display sim register	463
sim register enable	463
sim register server	464
sim register ssl-client-policy	464
New feature: Configuring TCP congestion control algorithm for TCP proxy	465
Configuring TCP congestion control algorithm for TCP proxy	465
Command reference	466
tcp-proxy congestion-method	466
New feature: Specifying the longest match principle for next hop recursion	467
Specifying the longest match principle for next hop recursion	467
Command reference	469
nexthop recursive-lookup longest-match	469
New feature: Configuring POS application load sharing and FEP group backup	470
Configuring a POS application template group	470
Command reference	471
display posa load-sharing statistics	471
posa app-group	472
reset posa load-sharing statistics	473
New feature: Disabling BGP from flushing specific routes to the routing table	473
Disabling BGP from flushing specific routes to the routing table	473
Command reference	474
routing-table bgp-rib-only	474
New feature: Configuring the POS application connection keep feature	475
Configuring the POS application connection keep feature	475
Command reference	476
posa app-connection keep	476
New feature: RIR-SDWAN	477
Configuring RIR-SDWAN	477
Enabling the RIR-SDWAN service	477
Enabling RIR to concern bandwidth when performing link selection	477
Specifying link preference values for links	478
Enabling the device to preferentially select links of the same transport network	478
Establishing RIR collaboration relationship between the local and peer devices	478
Associating a local SDWAN extended tunnel interface with a peer SDWAN tunnel interface	479
Synchronizing TTE connection and RIR link quality information of the local SDWAN tunnel interface to the peer device through the collaboration channel	479
Configuring a redirect IP address for RIR data packets	480
Configuring an interface RIR collaboration group ID	480
Configuring the aging timer for the TTE connection synchronized through the collaboration channel after it is disconnected	480
Enabling BFD for a tunnel	481
Configuring application quality detection	481
Command reference	482
New command: application-quality	482
New command: cqi-weight	483
New command: delay threshold	484
New command: display rir sdwan application-quality	485
New command: display rir sdwan bandwidth tunnel	487
New command: display rir sdwan flow	488
New command: display rir sdwan link-quality	489
New command: display rir sdwan session-statistics tunnel	491
New command: display sdwan collaboration channel	492
New command: instance	494

New command: link-select same-transport-network prefer	495
New command: link-bandwidth ignore	495
New command: link-quality probe interval	496
New command: path sdwan	497
New command: peer	497
New command: probe flow	498
New command: probe interval (application quality detection instance view)	499
New command: rir redirect group	500
New command: rir redirect peer	501
New command: rir sdwan	502
New command: signature	502
New command: sdwan collaboration peer	504
New command: sdwan collaboration peer-device-id	505
New command: sdwan collaboration tte-connection aging	506
New command: sdwan collaboration-map peer-device-id peer-interface-id	506
New command: tunnel bfd enable	507
New feature: SaaS path optimization	508
SaaS path optimization	508
SaaS applications	508
Methods for accessing SaaS applications	508
SaaS path quality probe	509
SaaS path quality evaluation	510
SaaS path optimization mechanism	511
Prerequisites for SaaS path optimization	511
SaaS path optimization tasks at a glance	511
Configuring network parameters for SaaS path optimization	512
Creating the SaaS path optimization view	512
Specifying a node type for the device	512
Specifying an interface for the device to directly access SaaS applications	513
Configuring SaaS application instances	513
Creating a SaaS application instance	513
Adding access URLs for a SaaS application	514
Configuring the health check URL for a SaaS application	514
Configuring the expected quality values for paths accessing a SaaS application	515
Configuring the CQI parameters	515
Matching only packets in the public network or specific VPN instances for SaaS path optimization	516
Command reference	516
New command: access-network	516
New command: application-instance	517
New command: cqi-weight (SaaS application instance view)	518
New command: direct interface	520
New command: display saas attribute	520
New command: display saas optimal-path	524
New command: display saas path-cqi	525
New command: display saas path-quality	526
New command: expect-quality	528
New command: health-url	529
New command: node-type	530
New command: saas-path-optimize	531
New command: url	532
New feature: Specifying a VXLAN tunnel as a dedicated link for a flow template	533
Specifying a VXLAN tunnel as a dedicated link for a flow template	533
Command reference	534
New command: rir dedicated flow	534
New feature: Enabling the device to drop service flows upon failure to find an optimal link	535
Enabling the device to drop service flows upon failure to find an optimal link	535

Command reference	536
New command: no-optimal-link drop	536
no-optimal-link drop	536
New feature: Configuring FEC optimization parameters	537
Configuring FEC optimization parameters	537
Command reference	537
fec loss-recovery-type	537
fec probe aging-time	538
fec sample-interval	539
New feature: Specifying the 5G NR network mode for the 5G modem to register with	540
Specifying the 5G NR network mode for the 5G modem to register with	540
Command reference	540
nr mode	540
New feature: Configuring TCP packet compression or decompression	541
Configuring TCP packet compression or decompression	541
Command reference	541
display waas statistics tcp compress	541
reset waas statistics tcp compress	542
waas tcp	542
waas tcp destination	543
New feature: Preferring routes learned from a peer or peer group during optimal route selection	544
Preferring routes learned from a peer or peer group during optimal route selection	544
Command reference	547
peer high-priority	547
New feature: Configuring the BGP Additional Paths feature	548
Configuring the BGP Additional Paths feature	548
Command reference	550
additional-paths select-best	550
peer additional-paths	551
peer advertise additional-paths best	552
New feature: Allowing the RR to change the attributes of routes to be reflected	554
Allowing the RR to change the attributes of routes to be reflected	554
Command reference	555
reflect change-path-attribute	555
New feature: Configuring packet duplication optimization	556
Configuring packet duplication optimization	556
Command reference	556
New command: display waas statistics packet-dup	556
Modified command: optimize	558
New command: reset waas statistics packet-dup	558
New feature: Specify an ACL to match the TCP or UDP packets that can be compressed or decompressed	559
Specify an ACL to match the TCP or UDP packets that can be compressed or decompressed	559
Command reference	559
waas tcp acl	559
waas udp acl	560
New feature: Configuring packet duplication parameters	561
Configuring packet duplication optimization parameters	561

About this task	561
Restrictions and guidelines	561
Enabling packet duplication RIR	562
Manually specifying a packet duplication path in an SDWAN network	562
Setting the packet duplication reorder timeout timer	562
Command reference	563
packet-dup reorder timeout	563
packet-dup rir enable	563
reset waas statistics load-balance	564
waas packet-dup sdwan static-path	565
New feature: Setting the reorder timeout timer for load balancing packets	566
Setting the reorder timeout timer for load balancing packets	566
Command reference	567
display waas statistics load-balance	567
waas load-balance reorder timeout	568
New feature: Support for the link tag feature	569
Configuring the IPv6 IS-IS link tag feature	569
Command reference	570
isis ipv6 link-tag	570
link-tag inherit enable	570
Configuring the OSPFv3 link tag feature	571
Command reference	572
link-tag inherit enable	572
ospfv3 link-tag	573
Modified feature: Binding a POS terminal template to an interface and configuring a POS application mapping entry	574
Feature change description	574
Command changes	574
Modified command: posa bind terminal	574
Modified command: posa map	575
Modified feature: Configuring RIR in RIR-SDWAN view, RIR-SDWAN flow template view, and RIR-SDWAN SLA view	575
Feature change description	575
Command changes	576
Modified command: flow priority-based-schedule bandwidth-threshold	576
Modified command: flow	576
Modified command: link-select delay	577
Modified command: expect-bandwidth	577
Modified command: flow priority-based-schedule enable	578
Modified command: flow priority-based-schedule schedule-period	578
Modified command: link-select suppress-period	579
Modified command: load-balance per-packet enable	579
Modified command: load-balance per-session periodic-adjust adjust-interval	580
Modified command: load-balance per-session periodic-adjust enable	580
Modified command: load-balance per-session periodic-adjust threshold	581
Modified command: log enable	581
Modified command: jitter threshold	582
Modified command: packet-loss threshold	582
Modified command: probe connect	582
Modified command: quality-policy	583
Modified command: sla	584
Modified command: Enabling BFD for LSPs associated with an FEC	584
Feature change description	584
Command changes	584
Modified command: mpls bfd (for LSP)	584

Displaying information about specific SR-MPLS TE or SRv6 TE policies ..	585
Feature change description	585
Command changes	585
Modified command: display bgp link-state	585
Modified feature: Displaying session statistics for the specified flow template	586
Feature change description	586
Command changes	586
Modified command: display rir sdwan session-statistics tunnel	586
Modified feature: Configuring preference for a link specified by its the SDWAN tunnel group ID in the flow template	587
Feature change description	587
Command changes	587
Modified command: path sdwan	587
Modified feature: Configuring FEC optimization parameters	588
Feature change description	588
Command changes	588
Modified command: fec average-ratio	588
Modified command: fec block-size	588
Modified command: fec decode-timeout	589
Modified command: fec encode-timeout	589
Modified command: match udp	589
Modified command: optimize	591
Modified feature: Displaying unicast routing information generated based on the Priority-Color extended community attribute	591
Feature change description	591
Command changes	592
Modified command: display bgp routing-table ipv4 unicast	592
Modified command: display bgp routing-table ipv6 unicast	592
Modified feature: Specifying a TCP congestion control algorithm for the WAN side	593
Feature change description	593
Command changes	593
Modified command: waas tfo congestion-method	593
Modified feature: RIR support for VPDN links	593
Feature change description	593
Command reference	594
Modified command: path link-type index preference	594
Modified command: rir link-type index	594
Modified feature: Using the original cost of redistributed routes	595
Feature change description	595
Command changes	595
Modified command: import-route (OSPF view)	595
Modified command: import-route (IS-IS view)	596
Modified command: import-route (OSPFv3 view)	598
Modified feature: Configuring IS-IS to redistribute user network routes and redistribute routes without keeping their SR labels	598
Feature change description	599
Command changes	599
Modified command: import-route	599

Modified feature: Setting the speed of an Ethernet interface	601
Feature change description	601
Command changes	601
Modified command: speed	601
Modified feature: Configuring load sharing for link aggregation groups based on flow labels	602
Feature change description	602
Command changes	602
Modified command:	602
Modified command:	602
Modified command:	603
Modified command:	603
Modified command: link-aggregation global load-sharing mode	604
Modified command: link-aggregation load-sharing mode	604
Modified feature: QinQ support for new views and keywords	605
Feature change description	605
Command changes	605
Modified command: qinq enable	605
Modified command: qinq ethernet-type (interface view)	605
Modified command: qinq ethernet-type (system view)	606
Modified feature: QinQ support for new keywords	606
Feature change description	606
Command changes	606
Modified command: qinq ethernet-type (interface view)	606
Modified command: qinq ethernet-type (system view)	607
Modified feature: Recursing an IPv6 static route to the specified SRv6 TE policy	607
Feature change description	607
Command changes	607
Modified command: ipv6 route-static	607
Modified feature: Recursing a static route to the specified SRv6 TE policy	608
Feature change description	608
Command changes	608
Modified command: ip route-static and ip route-static vpn-instance	608
Modified feature: Support for specifying a BJCA server for an AAA private-protocol scheme	609
Feature change description	609
Command changes	609
Modified command: authentication-server	609
Modified feature: Support of configuring an AAA private protocol scheme for IKE extended authentication	610
Feature change description	610
Command changes	610
Modified command: authorization ike	610
Modified feature: Support of displaying IPv4 unicast routing information generated based on the Priority-Color extended community attribute for a BGP-VPN instance routing table	611
Feature change description	611
Command changes	611
Modified command: display bgp routing-table vpnv4	611

Modified feature: Configuring the parameters carried in the URL of a portal Web server	611
Feature change description	611
Command changes	612
Modified command: url-parameter	612
Modified feature: Change of default values for the single-hop BFD detection time multiplier and Sbfd detection time multiplier	612
Feature change description	612
Command changes	612
Modified command: bfd detect-multiplier (BFD)	612
Modified command: bfd detect-multiplier (SBFD)	613
Modified feature: Displaying VRRP version information in the output from the display vrrp command	613
Feature change description	613
Command changes	613
Modified command: display vrrp	613
Modified feature: Configuring the parameters carried in the URL of a portal Web server	614
Feature change description	614
Command changes	615
Modified command: url-parameter	615
Modified command: display portal web-server	615
Modified feature: Using the gateway IP address obtained from the DHCP server through the specified interface as the next hop IP address for probe packets	616
Feature change description	616
Command changes	617
Modified command: next-hop	617
Modified feature: Specifying the aging parameters for dynamic flows	617
Feature change description	617
Command changes	617
Modified command: dynamic-flow aging-time	617
Modified feature: Specifying the measurement period for an iFIT instance	618
Feature change description	618
Command changes	618
Modified command: period	618
Modified feature: Binding additional analyzers to a collector instance	618
Feature change description	618
Command changes	618
Modified command: analyzer	618
Modified feature: Binding an MP to an interface	619
Feature change description	619
Command changes	619
Modified command: inqa mp	619
Modified feature: Specifying the length of probe packets for a tracer operation	620
Feature change description	620
Command changes	620
Modified command: tracer	620

Modified feature: Specifying the source IPv6 address of the probe packets for an IPv6 tracer operation	620
Feature change description	620
Command changes	621
Modified command: <code>tracert ipv6</code>	621
Modified feature: Setting the flow log version	621
Feature change description	621
Command changes	621
Modified command: <code>userlog flow export version</code>	621
Modified feature: Filtering the output from a display command with a regular expression	622
Feature change description	622
Command changes	622
Modified command: <code>display { { begin exclude include } }</code>	622
Modified feature: Configuring the NAT device to ignore the protocol packet type	622
Feature change description	622
Command changes	622
Modified command: <code>display nat all</code>	622
Modified command: <code>display nat static</code>	623
Modified command: <code>nat static inbound</code>	623
Modified command: <code>nat static outbound</code>	624
Modified feature: Static port blocks for AFT	624
Feature change description	624
Command changes	624
New command: <code>aft log port-block</code>	624
New command: <code>aft v6tov4 source port-block-group</code>	625
New command: <code>block-size</code>	627
New command: <code>ip-address</code>	627
New command: <code>ipv6-prefix</code>	628
New command: <code>port-range</code>	629
Modified command: <code>display aft configuration</code>	630
Modified command: <code>display aft port-block</code>	630
New feature: Support of URL-based automatic configuration for encryption	631
New feature: Support of USB-based automatic configuration for encryption	631
New feature: Configuring DNS redirection	632
Configuring DNS redirection	632
Command reference	632
New command: <code>dns redirect enable</code>	632
New feature: Enabling DNS server health check	633
Enabling DNS server health check	633
Command reference	634
New command: <code>health-check enable</code>	634
New feature: Disabling receiving a specific type of ICMPv6 messages	635
Disabling receiving a specific type of ICMPv6 messages	635
Command reference	635
<code>ipv6 icmpv6 receive enable</code>	635

New feature: Disabling sending a specific type of ICMPv6 messages	637
Disabling sending a specific type of ICMPv6 messages	637
Command reference	638
ipv6 icmpv6 send enable	638
New feature: Enabling advertising invalid delegated prefixes	639
Enabling advertising invalid delegated prefixes	639
Command reference	640
ipv6 nd ra invalid-delegated-prefix advertise enable	640
New feature: Setting the TTL value for DNS entries	641
Setting the TTL value for DNS entries	641
Command reference	642
New command: dns cache ttl	642
New feature: Configuring DNS filtering	643
Configuring DNS filtering	643
Command reference	644
New command: dns filter	644
New feature: Configuring DNS snooping	645
Configuring DNS snooping	645
Command reference	645
New command: dns snooping enable	645
New feature: Configuring the DNS transparent proxy	646
Configuring the DNS transparent proxy	646
Command reference	647
New command: dns transparent-proxy enable	647
Modified feature: Displaying the running configuration	648
Feature change description	648
Command changes	649
Modified command: display current-configuration	649
Modified feature: Displaying the contents of the configuration file for the next system startup	649
Feature change description	649
Command changes	650
Modified command: display saved-configuration	650
Modified feature: Displaying the running configuration in the current view	650
Feature change description	650
Command changes	650
Modified command: display this	650
Modified feature: Configuring an ACL match criterion	651
Feature change description	651
Command changes	651
Modified: if-match	651
Modified feature: Adding a node to a SID list	652
Feature change description	652
Command changes	652
Modified command: index	652
Modified feature: Configuring a traffic redirection action	653
Feature change description	653
Command changes	653
Modified: redirect	653

Modified feature: Clearing forwarding statistics for all SRv6 TE policies ..	653
Feature change description	653
Command changes	654
Modified: reset segment-routing ipv6 te forwarding statistics	654
Modified feature: Enabling Router ID filtering	654
Feature change description	654
Command reference	654
Modified command: router-id filter	654
Modified feature: Support of the ipv6 route-static command for the gateway keyword	655
Feature change description	655
Command changes	655
Modified command: ipv6 route-static	655
New feature: License installation and AC configuration	657
Feature description	657
New feature: Configuring bandwidth guaranteeing	657
Feature description	657
New feature: Enabling NetStream sampling for an SRv6 TE policy	658
Enabling NetStream sampling for an SRv6 TE policy	658
Command reference	658
New command: ip netstream outbound sampler srv6-policy	658
New feature: Enabling NetStream for an SRv6 TE policy	659
Enabling NetStream for an SRv6 TE policy	659
Command reference	660
New command: ip netstream outbound srv6-policy	660
New feature: Enabling IPv6 NetStream sampling for an SRv6 TE policy ..	660
Enabling IPv6 NetStream sampling for an SRv6 TE policy	660
Command reference	661
New command: ipv6 netstream outbound sampler srv6-policy	661
New feature: Enabling IPv6 NetStream for an SRv6 TE policy	662
Enabling IPv6 NetStream for an SRv6 TE policy	662
Command reference	662
New command: ipv6 netstream outbound srv6-policy	662
New feature: Importing the carrier address library at the GUI	663
Importing the carrier address library	663
New feature: Configuring the time zone at the GUI	663
Configuring the time zone at the GUI	663
New feature: Enabling Web logging	664
Enabling Web logging	664
Modified feature: Specifying multiple NTP servers	664
Feature change description	664
Modified feature: Flow-mirroring traffic to an interface	664
Feature change description	664
Command changes	665
Modified command: mirror-to interface	665

New feature: EoGRE	665
New feature: Configuring ARP attack detection on the Web interface	666
About this task	666
New feature: Configuring NAT address pools on the Web interface	666
About this task	666
New feature: Configuring application services on the Web interface	666
About this task	666
Static DNS	666
Dynamic DNS	666
New feature: Configuring a PCE	667
Configuring a PCE	667
Command reference	667
pce-client	667
pce capability segment-routing	668
New feature: Configuring stateful PCE on a PCC	668
Configuring stateful PCE on a PCC	668
Command reference	670
pce multi-delegate enable	670
pce retain initiated-lsp	671
pce retain lsp-state	672
New feature: Configuring PCEP session parameters	673
Configuring PCEP session parameters	673
Command reference	674
pce peer keychain	674
pce peer md5	674
New feature: Displaying local PCEP session settings and stateful PCE peers information	675
Displaying local PCEP session settings and stateful PCE peers information	675
Command reference	676
display mpls te pce parameter	676
display mpls te pce stateful neighbor	678
Modified feature: Configuring a NAT port mapping	679
Feature change description	679
Modified feature: Enabling BFD for LSPs associated with an FEC	679
Feature change description	679
Command changes	679
Modified command: mpls bfd (for LSP)	679
Modified feature: Displaying LSP information	680
Feature change description	680
Command changes	680
Modified command: display mpls lsp	680
Modified feature: Configuring a preferred tunnel in a tunnel policy	681
Feature change description	681
Command changes	681
Modified feature: preferred-path	681
Modified feature: Binding tunnels to a destination IP address in a tunnel policy	681
Feature change description	681

Command changes	682
Modified command: binding-destination	682
New feature: Reserving an MPLS TE tunnel for tunnel binding policies	682
Reserving an MPLS TE tunnel for tunnel binding policies	682
Command reference	682
mpls te reserved-for-binding	682
Modified feature: Configuring one-to-one mappings on the Web interface	683
Feature change description	683
Modified feature: Support of configuring Option 82 on a VEB interface	683
Feature change description	683
Command changes	685
Modified command: dhcp snooping information circuit-id	685
Modified command: dhcp snooping information enable	686
Modified command: dhcp snooping information remote-id	687
Modified command: dhcp snooping information strategy	687
Modified feature: Configuring a private address-to-public address mapping for an NHS of mGRE	688
Feature change description	688
Command changes	688
Modified command: nhrp nhs	688
Modified feature: Support for configuring Web Cache for devices in the RIR-SDWAN scenario	688
Feature change description	688
New feature: Configuring optimized features for HTTP proxy	689
About HTTP proxy	689
Working mechanism	689
External link proxy	692
License requirement for HTTP proxy	694
HTTP proxy tasks at a glance	694
Configuring a Web server group	695
Configuring an HTTP proxy service	696
Specifying an SSL certificate file and SSL certificate key file	697
About specifying an SSL certificate file and SSL certificate key file	697
Restrictions and guidelines	697
Prerequisites	697
Specifying an SSL certificate file and SSL certificate key file	698
Specifying a domain-specific SSL certificate file and SSL certificate key file	698
Configuring the external link proxy feature	699
About configuring the external link proxy feature	699
Prerequisites	699
Configuring the external media link proxy feature	699
Configuring the external hyperlink proxy feature	700
Configuring the external link reference feature	700
Configuring the advanced features for an HTTP proxy service	701
Configuring a source IP pool used for Web server connection	701
Enabling caching of Web server resources	701
Specifying a keyword to be monitored and a keyword to replace the monitored keyword	702
Enabling referer protection	703
Enabling URL protection	703
Enabling an HTTP proxy service	704
Configuring the HTTP proxy operation recording	704
Display and maintenance commands for HTTP proxy in an HTTP proxy service view	705
Command reference	705
Modified command: access-record enable	705
New command: access-record max-size	706

New command: cache-data	707
New command: denylist-domain-name	708
Modified command: display http-proxy	709
New command: display http-proxy monitor-info	712
Modified command: dns-server	713
Modified command: domain-name	714
New command: exclude-external-domain	715
New command: extlink-href enable	716
Modified command: hyperlink-proxy	717
New command: keyword monitor	717
Modified command: medialink-proxy enable	718
New command: referer-protection enable	719
New command: ssl certificate directory	720
New command: ssl certificate domain-name file key-file	721
New command: url-protection enable	722
New command: wildcard-domain-name	723
New command: display system internal http-proxy service fail	724
New feature: Configuring HTTP proxy in an HTTP proxy server view	725
Configuring HTTP proxy in an HTTP proxy server view	725
Restrictions and guidelines: HTTP proxy in an HTTP proxy server view	725
HTTP proxy tasks at a glance	725
Creating an HTTP proxy server view	726
Configuring proxy-related parameters in an HTTP proxy server view	726
Specifying an SSL certificate file and SSL certificate key file	727
Configuring the external link proxy feature	727
About configuring the external link proxy feature	727
Restrictions and guidelines	728
Prerequisites	728
Configuring the external link reference feature	728
Configuring the external hyperlink proxy feature	728
Configuring the advanced features in an HTTP proxy server view	729
Configuring a source IP pool used for Web server connection	729
Enabling caching of Web server resources	729
Specifying a keyword to be monitored and a keyword to replace the monitored keyword	730
Enable referer protection	730
Enabling URL protection	730
Deleting response header set-cookie attributes	730
Enabling the restoration of QueryString in Web requests	731
Replacing an HTTP or HTTPS response header or restoring an HTTP or HTTPS request header	732
Configuring a redirect URL domain name that allows replacement	733
Referencing an HTTP proxy server view	733
Enabling wildcard domain name encryption feature for an HTTP proxy service	734
Configuring the HTTP proxy operation recording	735
Enabling an HTTP proxy service	735
Display and maintenance commands for HTTP proxy in an HTTP proxy server view	735
Command reference	736
Modified command: cache-data	736
New command: delete cookie-flag	736
Modified command: denylist-domain-name	738
Modified command: display http-proxy	738
New command: display http-proxy server	739
Modified command: domain-name	741
Modified command: exclude-external-domain	743
New command: extlink-encryption algorithm	743
Modified command: extlink-href enable	744
Modified command: failed-extlink inform	745
Modified command: failed-extlink redirect	746
Modified command: http-proxy server-group	746
New command: http-proxy server	747
Modified command: hyperlink-proxy	747
New command: include-external-domain	748

New command: include-redirect-domain	749
New command: include server	750
Modified command: ipv6-address	751
Modified command: medialink-proxy enable	751
Modified command: protocol-type (http proxy service view)	752
New command: protocol-type (HTTP proxy server view)	752
New command: referer-protection domain	753
New command: replace response-header	755
New command: restore request-header	756
New command: restore request-querystring	757
Modified command: ssl certificate domain-name file key-file	758
New feature: Support for proxy NTLM authentication packets and obtaining the suffix of a Web cache file from the PMO website URL	759
Configuring extended Web caching features	759
Enabling Web caching for files in QueryString of a URL	759
Configuring Web caching to ignore the specified HTTP/HTTPS response headers	759
Command reference	760
New command: cache-ignore	760
New command: querystring-file-cache enable	761
New feature: Enhancing tunnel maintenance	762
Command reference	762
New command: debugging system internal tunnel trace	762
Modified command: display system internal tunnel data	762
New command: display system internal tunnel kernel global run-info	763
New command: display system internal tunnel statistics	764
New command: display system internal tunnel table	764
New command: display system internal tunnel wait-list	765
New command: reset system internal tunnel statistics	766
Modified command: debugging tunnel	766
New feature: Configuring dual-device backup for Web caching	768
Configuring Web caching backup	768
Web caching backup	768
Configuring Web caching backup	768
Command reference	769
New command: dual-gateway-channel	769
New feature: Enabling HTTPS-based Web caching	770
Enabling HTTPS-based Web caching	770
Specify listening port numbers	770
Command reference	771
New command: https enable	771
New command: https listen-port	772
Modified command: listen-port	772
New feature: ADVPN support specifying the link protocol type of the hub ·	773
Configuring hub groups	773
Command reference	775
Modified command: hub ipv6 private-address	775
Modified command: hub private-address	776
New feature: GRE keepalive support for the reply-check-only mode	778
Configuring a GRE/IPv4 tunnel	778
Command reference	780
Modified command: keepalive	780
Modified command: display interface tunnel	780
New feature: eMDI	781
About eMDI	781

eMDI implementation	781
Monitored items	782
Restrictions: Hardware compatibility with eMDI	785
Restrictions and guidelines	787
Prerequisites	787
Configuring eMDI	787
Configuring an eMDI instance	787
Starting an eMDI instance	788
Stopping an eMDI instance	789
Display and maintenance commands for eMDI	789
Command reference	790
alarm suppression times	790
alarm threshold	791
description	792
display emdi instance	792
display emdi resource	795
display emdi statistics	796
emdi	801
fec	802
flow ipv4 tcp	803
flow ipv4 udp	804
instance	805
lifetime	806
monitor-period	807
monitor-period-packet maximum	807
reset emdi statistics	808
start	809
stop	809
stop all	810
New feature: Enabling SNMP notifications for OpenFlow	810
Enabling SNMP notifications for OpenFlow	810
Command reference	810
New command: snmp-agent trap enable openflow	810
New feature: EVPN VPLS	811
About EVPN VPLS	811
EVPN VPLS network model	811
Neighbor auto-discovery and PW establishment	812
MAC address learning, aging, and withdrawal	812
Traffic forwarding and flooding	813
Full mesh and split horizon	813
EVPN VPLS multihoming	813
ARP flood suppression	816
Control word	817
MAC mobility	818
EVPN E-tree	818
EVPN VPLS tasks at a glance	819
(Optional.) New feature: Error code detection	819
Configuring error code detection	错误!未定义书签。
About error code detection	错误!未定义书签。
Error code detection fundamentals	错误!未定义书签。
Error code detection deployment	错误!未定义书签。
Restrictions and guidelines: Error code detection configuration	错误!未定义书签。
Configuring interface error code detection	错误!未定义书签。
Configuring link quality detection	错误!未定义书签。
Configuring the bit error ratio calculation factors for an interface	错误!未定义书签。
Display and maintenance commands for error code detection	错误!未定义书签。
Command reference	错误!未定义书签。
crc-error bit-error-ratio algorithm-parameter	错误!未定义书签。

display ifmonitor	错误!未定义书签。
link-quality crc-error bit-error-ratio	错误!未定义书签。
port ifmonitor crc-error bit-error-ratio	错误!未定义书签。
reset crc-error bit-error-ratio status interface	错误!未定义书签。
Modified feature: Local FPGA mirroring group	错误!未定义书签。
Feature change description	错误!未定义书签。
Command changes	错误!未定义书签。
Modified command: mirroring-group	错误!未定义书签。
Modified command: mirroring-group mirroring-port (interface view)	错误!未定义书签。
Modified command: mirroring-group mirroring-port (system view)	错误!未定义书签。
Modified command: mirroring-group monitor-port (interface view)	错误!未定义书签。
Modified command: mirroring-group monitor-port (system view)	错误!未定义书签。
Modified command: display mirroring-group	错误!未定义书签。
Modified feature: Configuring a match criterion for QoS	错误!未定义书签。
Feature change description	错误!未定义书签。
Command changes	错误!未定义书签。
Modified command: if-match	错误!未定义书签。
Modified feature: Support for keychain authentication with the HMAC-SM3 or SM3 algorithm	错误!未定义书签。
Feature change description	错误!未定义书签。
Command changes	错误!未定义书签。
Modified command: authentication-algorithm	错误!未定义书签。
Modified command: tcp-algorithm-id	错误!未定义书签。
Modified feature: Configuring a static route	错误!未定义书签。
Feature change description	错误!未定义书签。
Command changes	错误!未定义书签。
Modified command: ip route-static	错误!未定义书签。
Modified command: ip route-static vpn-instance	错误!未定义书签。
Restrictions and guidelines: EVPN VPLS configuration	820
Configuring a VSI	820
Creating a VSI	820
Configure VSI parameters	820
Configuring an EVPN instance	821
Mapping a Layer 3 interface to a VSI	822
Configuring BGP to advertise BGP EVPN routes	823
Restrictions and guidelines for BGP EVPN route advertisement	823
Enabling BGP to advertise BGP EVPN routes	823
Enabling advertisement of MPLS-encapsulated BGP EVPN routes	823
Configuring optimal route selection and route advertisement settings	824
Maintaining BGP sessions	825
Configuring a PW class	825
Configuring EVPN VPLS multihoming	826
Restrictions and guidelines for EVPN VPLS multihoming	826
Assigning an ESI to an interface	826
Configuring the DF election algorithm	827
Setting the DF election delay	828
Setting the advertisement delay timer for Ethernet auto-discovery routes	828
Configuring local FRR for EVPN VPLS	829
Generating MAC address entries for received MAC/IP advertisement routes	830
Enabling VSIs to ignore the state of ACs	830
Disabling advertisement of EVPN multihoming routes	831
Ignoring the Ethernet tag on advertisement of Ethernet auto-discovery and MAC/IP advertisement routes	831
Enabling the device to monitor the BGP peer status of another local edge device	832

Managing remote MAC address entries and remote ARP learning	833
Disabling MAC address advertisement	833
Disabling learning of MAC addresses from ARP information	833
Disabling ARP information advertisement	834
Enabling EVPN E-tree	834
Confining floods to the local site	835
Enabling ARP flood suppression	835
Enabling packet statistics for an AC	836
Restrictions and guidelines for AC packet statistics	836
Enabling packet statistics for a Layer 3 interface	836
Enabling SNMP notifications for L2VPN PWs	836
Display and maintenance commands for EVPN VPLS	837
Command reference	838
arp-advertising disable	838
display evpn es	839
display evpn df-election	845
display evpn instance	847
display l2vpn forwarding evpn	850
display l2vpn forwarding evpn split-horizon	852
e-tree enable	854
evpn df-election algorithm (interface view)	855
evpn df-election algorithm (system view)	856
evpn df-election preference	856
evpn df-election preference non-revertive	857
evpn frr local (EVPN instance view/VSI EVPN instance view)	858
evpn multihoming advertise disable	859
evpn multihoming advertise ignore-ethernet-tag	859
evpn multihoming vpls-frr local	860
evpn multihoming re-originated mac	861
evpn multihoming timer df-delay	862
evpn timer ad-delay	862
evpn timer es-delay	863
evpn track peer	864
ignore-ac-state	865
l2vpn ignore-ac-state	866
pw-class	867
tunnel-policy	867
Modified command: display evpn auto-discovery	868
Modified command: display evpn route mac	868
Modified command: evpn encapsulation	869
New feature: EVPN VPWS	869
About EVPN VPWS	869
EVPN VPWS network model	870
Remote connection establishment	870
EVPN VPWS multihoming	871
FRR for EVPN VPWS	874
Control word	875
PW concatenation	875
Inter-AS communication of EVPN VPWS	876
LDP or static PW ACs for EVPN PWs	879
EVPN VPWS tasks at a glance	879
Configuring a remote connection	879
Configuring PW concatenation	880
Restrictions and guidelines: S-trunk support	880
Prerequisites for EVPN VPWS	880
Enabling L2VPN	880
Configuring a Layer 3 interface with Ethernet or VLAN encapsulation	881
Configuring EVPN route advertisement	881
Restrictions and guidelines for EVPN route advertisement configuration	881
Enabling BGP to advertise BGP EVPN routes	881
Enabling the device to advertise MPLS-encapsulated BGP EVPN routes	882

Configuring optimal route selection and route advertisement settings	882
Maintaining BGP sessions	884
Configuring a cross-connect	884
Configuring a PW	884
Configuring a PW class	884
Configuring an EVPN PW	885
Mapping an AC to a cross-connect	886
About mapping an AC to a cross-connect	886
Restrictions and guidelines for mapping an AC to a cross-connect	886
Mapping a Layer 3 interface to a cross-connect	886
Configuring EVPN VPWS multihoming	887
Restrictions and guidelines for EVPN VPWS multihoming	887
Assigning an ESI to an interface	887
Configuring the DF election algorithm	888
Setting the redundancy mode on an interface	889
Setting the DF election delay	890
Disabling advertisement of EVPN multihoming routes	890
Enabling the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes	891
Enabling the device to monitor the BGP peer status of another local edge device	891
Configuring FRR for EVPN VPWS	892
Configuring local FRR	892
Configuring remote FRR	893
Configuring LDP or static PWs as ACs for EVPN PWs	893
About LDP or static PW AC configuration for EVPN PWs	893
Restrictions and guidelines for LDP or static PW AC configuration for EVPN PWs	894
Prerequisites for LDP or static PW AC configuration for EVPN PWs	894
Configuring an LDP PW as an AC for an EVPN PW	894
Configuring a static PW as an AC for an EVPN PW	895
Display and maintenance commands for EVPN VPWS	896
Command reference	898
ac interface	898
display evpn route xconnect-group	899
evpn frr local (cross-connect group EVPN instance view)	902
evpn frr remote	903
evpn local-service-id remote-service-id	903
evpn multihoming vpws-frr local	904
evpn redundancy-mode	905
New feature: EVPN VXLAN forwarding mode	906
Configuring the traffic forwarding mode for EVPN VXLAN	906
Command reference	907
evpn irb asymmetric	907
New feature: Enabling an ED to replace the L3 VXLAN ID, RD, and route targets of BGP EVPN routes	908
Enabling an ED to replace the L3 VXLAN ID, RD, and route targets of BGP EVPN routes	908
Command reference	909
peer advertise original-route	909
peer re-originated	910
peer suppress re-originated	911
New feature: Enabling EVPN to advertise VPN routes	912
Command reference	912
evpn mpls routing-enable	912
Modified feature: Displaying BGP EVPN route information with the specified prefix	913
Feature change description	913
Command changes	913
Modified command: display bgp l2vpn evpn	913

Modified feature: Saving the configuration in safe mode	914
Feature change description	914
New feature: Configuring MACsec	914
About MACsec	914
Basic concepts	915
MACsec services	915
MACsec application modes	916
MACsec operating mechanism	916
Protocols and standards	918
Restrictions: Hardware compatibility with MACsec	918
MACsec tasks at a glance	920
Enabling MKA	921
Enabling MACsec desire	921
Specifying the cipher suite for MACsec encryption	921
Configuring a preshared key	922
Configuring the MKA key server priority	922
Setting the MKA life time	923
Configuring MACsec protection parameters	923
About MACsec protection parameters	923
Restrictions and guidelines for MACsec protection parameter configuration	923
Configuring MACsec protection parameters in interface view	924
Configuring MACsec protection parameters by MKA policy	925
Enabling MKA session logging	926
Display and maintenance commands for MACsec	926
Troubleshooting MACsec	927
Cannot establish MKA sessions between MACsec devices	927
Command reference	927
confidentiality-offset	927
display macsec	928
display mka policy	930
display mka session	931
display mka statistics	934
macsec cipher-suite	935
macsec confidentiality-offset	936
macsec desire	937
macsec mka-session log enable	938
macsec replay-protection enable	938
macsec replay-protection window-size	939
macsec validation mode	940
mka apply policy	941
mka enable	942
mka policy	942
mka priority	943
mka psk	944
mka timer mka-life	945
replay-protection enable	946
replay-protection window-size	947
reset mka session	948
reset mka statistics	948
validation mode	949
New feature: Configuring the device as responder-only for IPsec SA negotiation	950
Configuring the device as responder-only for IPsec SA negotiation	950
Command reference	950
New command: responder-only enable	950
Modified command: display ipsec { ipv6-policy policy }	951
Modified command: display ipsec { ipv6-policy-template policy-template }	953
Modified command: display ipsec profile	954
Modified command: display ipsec statistics	955

New feature: Specifying a security enhanced level	955
Specifying a security enhanced level	955
Command reference	956
security-enhanced level	956
New feature: Configuring GD-quantum encryption	959
Configuring GD-quantum encryption	959
Command reference	962
app-dev-info (IKE GDQUANTUM view)	962
auth-key	964
decrypt-quantum-key	967
ike gd-quantum	969
server-address	972
New feature: Enabling SNMP notifications for PKI	974
Enabling SNMP notifications for PKI	974
Command reference	975
snmp-agent trap enable pki	975
New feature: Configuring the initiator to use dynamic source UDP ports for IKE negotiations	976
Configuring the initiator to use dynamic source UDP ports for IKE negotiations	976
Command reference	977
client source-udp-port dynamic	977
New feature: Binding a smart token to the device	978
Binding a smart token to the device	978
Hardware compatibility with smart token binding	978
Binding the smart token to a PKI domain	979
Specifying a user PIN code for the smart token	980
Command reference	980
bind smart-token	980
display pki smart-token	983
pki smart-token	985
New feature: Configuring the title for the PKI entity	988
Configuring the title for the PKI entity	988
Command reference	988
title	988
New feature: Configuring ZD-quantum encryption	989
Configuring ZD-quantum encryption	989
Command reference	991
app-dev-info (IKE ZD-quantum view)	991
ike zd-quantum	994
New feature: Setting a limit to the number of IKEv2 SAs	996
Setting a limit to the number of IKEv2 SAs	996
Command reference	997
ikev2 limit	997
Modified feature: Displaying information about IPsec SAs	997
Feature change description	997
Command changes	998
Modified command: display ipsec sa	998
Modified feature: Configuring a peer ID for IKE profile matching	1000
Feature change description	1000
Command changes	1000
Modified command: match remote	1000

Modified feature: Configuring a preshared key	1002
Feature change description	1002
Command changes	1002
Modified command: pre-shared-key	1002
Modified feature: Enabling ALG to process IP fragments and TCP segments	1003
Feature change description	1003
Command changes	1003
Modified command: session alg fragment	1003
Modified feature: Not support for DES, 3DES, MD5, RC4, and RC2 cipher suites in SSL client and server policies	1004
Feature change description	1004
Command changes	1004
Modified command: ciphersuite	1004
Modified command: prefer-cipher	1011
Modified feature: Not support for an SSL protocol version lower than TLS 1.1 for session negotiation	1019
Feature change description	1019
Command changes	1020
Modified command: ssl version disable	1020
Modified command: version	1031
Modified feature: Disabling SSL session renegotiation	1035
Feature change description	1035
Command changes	1035
Modified command: ssl renegotiation disable	1035
Modified feature: Displaying information about SDWAN IPsec tunnels	1039
Feature change description	1039
Command changes	1039
Modified command: display ipsec sdwan-tunnel	1039
Modified feature: Specifying the user information required for client authentication	1041
Feature change description	1041
Command changes	1041
Modified command: client-authentication xauth user	1041
Modified feature: Displaying information about IKE SAs	1042
Feature change description	1042
Command changes	1042
Modified command: display ike sa	1042
Modified feature: Displaying IKE statistics	1044
Feature change description	1044
Command changes	1044
Modified command: display ike statistics	1044
Modified feature: Displaying the IKEv2 SA information	1047
Feature change description	1047
Command changes	1047
Modified command: display ikev2 sa	1047
Modified feature: Displaying IKEv2 statistics	1047
Feature change description	1047
Command changes	1048

Modified command: display ikev2 statistics.....	1048
Modified feature: Support for the incremental increase in user locking period	
.....	1050
Feature change description.....	1050
Command changes	1050
Modified command: password-control login-attempt.....	1050
Release 6728P25.....	1050
Release 6728P20.....	1051
Release 6728P15.....	1051
Release 0821P11.....	1051
Release 0809P33.....	1051
Release 0809P32.....	1051
Release 0809P29.....	1051
Modified feature: Configuring an IPv6 static route.....	1051
Feature change description.....	1051
Command changes	1052
Modified command: ipv6 route-static	1052
Release 0809P27.....	1053
New feature: Configuring the DHCP-designated default router as the next hop of a static route	1053
Configuring the DHCP-designated default router as the next hop of a static route	1053
Command reference	1054
Modified command: ip route-static	1054
New feature: Source IP pools for outgoing packets sent by an HTTP proxy service	1055
Configuring source IP pools for outgoing packets sent by an HTTP proxy service	1055
Command reference	1055
ip-pool.....	1055
Modified feature: Displaying HTTP proxy configuration information	1056
Feature change description.....	1056
Command changes	1057
Modified command: display http-proxy.....	1057
Release 0707P24.....	1057
Modified feature: Processing for user IP conflicts on an LNS	1057
Feature change description.....	1057
Command changes	1057
New command: l2tp user-ip-conflict offline	1057
Modified feature: Login password control.....	1058
Feature change description.....	1058
Command changes	1058

Release 0707P21.....	1058
Release 0707P19.....	1058
Release 0707P16.....	1058
Modified feature: Ethernet interface.....	1058
Feature change description.....	1058
Command changes.....	1059
Modified command: display interface.....	1059
Release 0707P12.....	1059
New feature: RADIUS ACL assignment by ACL name.....	1060
Release 0615P16.....	1060
New feature: mGRE.....	1060
Overview.....	1060
mGRE operation scheme.....	1060
mGRE operation procedure.....	1061
mGRE support for NAT traversal.....	1063
mGRE configuration task list.....	1063
Configuring an mGRE tunnel.....	1063
Configuring routing.....	1064
Configuring IPsec for an mGRE tunnel.....	1065
Displaying and maintaining mGRE.....	1065
Command reference.....	1065
New command: display mgre session.....	1065
New command: display nhrp map.....	1069
New command: display nhrp statistics.....	1071
New command: nhrp authentication.....	1072
New command: nhrp holdtime.....	1073
New command: nhrp network-id.....	1074
New command: nhrp nhs.....	1074
New command: reset mgre session.....	1075
New command: reset mgre statistics.....	1076
New command: reset nhrp statistics.....	1076
New feature: Public key management support for Suite B.....	1077
Configuring Suite B in public key management.....	1077
Modified command: public-key local create.....	1077
New feature: PKI support for Suite B.....	1077
Configuring Suite B in PKI.....	1077
Modified command: public-key ecdsa.....	1077
New feature: IPsec support for Suite B.....	1078
Overview.....	1078
IKEv2 negotiation process.....	1078
New features in IKEv2.....	1079
Protocols and standards.....	1080
IKEv2 configuration task list.....	1080
Configuring an IKEv2 profile.....	1081
Configuring an IKEv2 policy.....	1083
Configuring an IKEv2 proposal.....	1084
Configuring an IKEv2 keychain.....	1085
Configure global IKEv2 parameters.....	1086
Enabling the cookie challenging feature.....	1086
Configuring the IKEv2 DPD feature.....	1086
Configuring the IKEv2 NAT keepalive feature.....	1087

Configuring IKEv2 address pools	1087
Displaying and maintaining IKEv2	1088
Command reference	1088
New command: aaa authorization	1088
New command: address	1089
New command: authentication-method	1090
New command: certificate domain	1091
New command: config-exchange	1092
New command: description	1093
New command: display ike statistics	1094
New command: display ikev2 policy	1094
New command: display ikev2 profile	1095
New command: display ikev2 proposal	1097
New command: display ikev2 sa	1098
New command: display ikev2 statistics	1102
New command: dh	1103
New command: dpd	1104
New command: encryption	1105
New command: hostname	1106
New command: identity	1107
New command: identity local	1108
New command: ikev2 address-group	1108
New command: ikev2 cookie-challenge	1109
New command: ikev2 dpd	1110
New command: ikev2 ipv6-address-group	1111
New command: ikev2 keychain	1112
New command: ikev2 nat-keepalive	1112
New command: ikev2 policy	1113
New command: ikev2 profile	1114
New command: ikev2 proposal	1115
New command: inside-vrf	1116
New command: integrity	1116
New command: keychain	1117
New command: match local (IKEv2 profile view)	1118
New command: match local address (IKEv2 policy view)	1119
New command: match remote	1120
New command: match vrf (IKEv2 policy view)	1121
New command: match vrf (IKEv2 profile view)	1122
New command: nat-keepalive	1123
New command: peer	1123
New command: pre-shared-key	1124
New command: prf	1126
New command: priority (IKEv2 policy view)	1127
New command: priority (IKEv2 profile view)	1127
New command: proposal	1128
New command: reset ikev2 sa	1129
New command: reset ikev2 statistics	1130
New command: sa duration	1130
New command: esn enable	1131
New command: ikev2-profile	1131
New command: tfc enable	1132
Modified command: ah authentication-algorithm	1133
Modified command: display ipsec { ipv6-policy policy }	1133
Modified command: display ipsec { ipv6-policy-template policy-template }	1134
Modified command: display ipsec sa	1134
Modified command: display ipsec transform-set	1134
Modified command: display ipsec tunnel	1135
Modified command: esp authentication-algorithm	1135
Modified command: esp encryption-algorithm	1136
Modified command: pfs	1137
Modified command: pre-shared-key	1137
Modified command: authentication-algorithm	1138

New feature: SSL support for Suite B	1139
Configuring Suite B in SSL.....	1139
Command reference	1139
New command: display crypto version.....	1139
New command: ssl version disable	1139
New command: ssl renegotiation disable	1140
Modified command: version.....	1141
Modified command: ciphersuite	1141
Modified command: prefer-cipher	1143
New feature: FIPS support for Suit B	1144
Configuring Suite B in FIPS.....	1144
Command reference	1144
New command: fips rng random size filename	1144
New command: fips rng random size round rate-statistics	1145
New command: fips rng entropy size filename	1146
New command: fips rng entropy size round rate-statistics	1146
New command: fips kdf	1147
New command: fips algorithm verify.....	1147
Modified command: fips self-test	1148
New feature: SSH support for Suite B	1148
Configuring SSH based on Suite B algorithms	1148
Specifying a PKI domain for the SSH server	1148
Establishing a connection to an Stelnet server based on Suite B	1149
Establishing a connection to an SFTP server based on Suite B	1149
Establishing a connection to an SCP server based on Suite B	1150
Specifying algorithms for SSH2.....	1150
Command reference	1152
New command: display ssh2 algorithm.....	1152
New command: ssh server pki-domain	1152
New command: scp ipv6 suite-b.....	1153
New command: scp suite-b	1155
New command: sftp ipv6 suite-b.....	1156
New command: sftp suite-b	1158
New command: ssh2 ipv6 suite-b	1159
New command: ssh2 suite-b	1161
New command: ssh2 algorithm cipher	1163
New command: ssh2 algorithm key-exchange	1164
New command: ssh2 algorithm mac	1165
New command: ssh2 algorithm public-key.....	1165
Modified command: display ssh server	1166
Modified command: ssh user	1167
Modified command: scp.....	1167
Modified command: scp ipv6	1170
Modified command: sftp.....	1172
Modified command: sftp ipv6	1175
Modified command: ssh2	1177
Modified command: ssh2 ipv6	1180
New command: fips kdf ssh.....	1182
New feature: EVPN	1183
Configuring EVPN	1183
Command reference	1183
New feature: SM2 key pair creation	1183
Creating an SM2 key pair	1183
Command reference	1183
New command: public-key local create sm2	1183

New feature: Built-in AC	1184
Configuring the built-in AC	1184
Command reference	1184
Release 0605P20.....	1184
Modified feature: Authentication mode for accessing a 4G network	1184
Feature change description	1184
Command changes	1185
Modified command: authentication-mode	1185
Release 0605P13.....	1185
New feature: Associating Track with a tracked list	1185
Associating Track with a tracked list	1185
Command reference	1185
New feature: Associating Track with EAA	1186
Associating Track with EAA	1186
Command reference	1186
event track	1186
Modified feature: Support for ACLs in SNMP commands	1188
Feature change description	1188
Command changes	1188
Modified command: snmp-agent community	1188
Modified command: snmp-agent group	1188
Modified command: snmp-agent usm-user	1189
Modified command: snmp-agent usm-user v3	1189
Modified feature: NAT for the multicast source address in PIM join and prune messages	1190
Feature change description	1190
Modified feature: Setting the maximum number of concurrent FTP users	1191
Feature change description	1191
Command changes	1191
Modified command: aaa session-limit ftp	1191
Modified feature: Portal authentication	1191
Feature change description	1191
Command changes	1191
Release 0415	1191
Release 0413	1191
New feature: IP forwarding last hop holding	1192
Configuring last hop holding	1192
Command reference	1192
ip last-hop hold	1192
Modified feature: Temporary user role authorization	1193
Feature change description	1193
Command changes	1193
Modified command: super password	1193

Release 0411	1193
Release 0410	1193
New feature: Support of multicast for ADVPN	1197
Configuring support of multicast for ADVPN	1197
Command reference	1197
New feature: Application layer state filtering	1198
Configuring application layer state filtering	1198
Command reference	1198
New feature: SIP keepalive	1198
Configuring SIP keepalive.....	1198
Command reference	1198
New command: options-ping	1198
New command: voice-class sip options-ping.....	1199
New feature: Multicast fast forwarding	1200
Configuring multicast fast forwarding	1200
Command reference	1200
New command: display multicast fast-forwarding cache.....	1200
New command: reset multicast fast-forwarding cache	1202
New command: display ipv6 multicast fast-forwarding cache	1203
New command: reset ipv6 multicast fast-forwarding cache	1204
New feature: SSL support for POS terminal access	1205
Configuring an SSL policy for POS terminal access	1205
Command reference	1206
New command: posa terminal ssl-server-policy.....	1206
Modified command: posa terminal	1207
New feature: Attack defense policy application to a security zone	1207
Applying an attack defense policy to a security zone.....	1207
Command reference	1207
New feature: AAA support for IKE extended authentication	1208
Configuring IKE extended authentication	1208
Command reference	1208
New feature: Percentage-based CAR	1208
Configuring percentage-based CAR	1208
Command reference	1208
New feature: Logging OSPF router ID conflict events	1209
Logging OSPF router ID conflict events.....	1209
Command reference	1209
New feature: AFT	1209
Configuring AFT	1209
Command reference	1209
New feature: Configuring enhanced CC authentication in FIPS mode.....	1210
Configuring enhanced CC authentication in FIPS mode	1210
Command reference	1210
New feature: Support of AAA for NETCONF	1210
Configuring support of AAA for NETCONF	1210
Command reference	1211

New feature: Mobile IP tunnel interface settings	1211
Configuring the mobile IP tunnel interface settings	1211
Command reference	1211
New feature: LISP	1212
Configuring LISP	1212
Command reference	1212
New feature: LISP tunnel entries and dynamic mobility	1212
Configuring LISP tunnel entries and dynamic mobility	1212
Command reference	1212
New feature: Support of IPv6 multicast routing for VPN instances	1213
Enabling support of IP multicast routing for VPN instances	1213
Command reference	1213
New feature: IPv4/IPv6 PIM NSR	1213
Enabling IPv4/IPv6 PIM NSR	1213
Command reference	1213
New feature: IGMP/MLD NSR	1213
Enabling IGMP/MLD NSR	1213
Command reference	1214
New feature: IPv4/IPv6 PIM passive mode	1214
Enabling IPv4/IPv6 PIM passive mode	1214
Command reference	1214
New feature: LISP virtual machine multi-hop mobility and DDT	1214
Configuring LISP virtual machine multi-hop mobility and DDT	1214
Command reference	1214
New feature: LISP NSR	1215
Configuring LISP NSR	1215
Command reference	1215
New feature: PPPoE client support for IPv6	1215
Associating a dial rule with a dialup interface	1215
Command reference	1215
Specifying an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address	1216
Command reference	1216
New feature: Frame-Relay-related functions	1216
Configuring multilink Frame Relay	1216
Command reference	1216
Configuring Frame Relay FRF.12 fragmentation	1216
Command reference	1216
Configuring Frame Relay STAC compression	1217
Command reference	1217
Configuring Frame Relay IPv6 address mapping	1217
Command reference	1217
Enabling SNMP notifications for Frame Relay	1217
Command reference	1218
Setting the Frame Relay interface type	1218
Command reference	1218
Configuring Frame Relay QoS	1218
Command reference	1218
New feature: DPI engine and content filtering	1218
Configuring the DPI engine and content filtering	1218
Command reference	1219

New feature: IPS	1219
Configuring IPS	1219
Command reference	1219
New feature: NBAR	1219
Configuring NBAR	1219
Command reference	1219
New feature: URL filtering	1220
Configuring URL filtering	1220
Command reference	1220
New feature: Local portal Web server	1220
Configuring a local portal Web server	1220
Command reference	1220
New feature: Support of portal for NETCONF	1221
New feature: Newly-added MIB objects	1221
New feature: Performing a loopback test	1221
Performing a loopback test	1221
Command reference	1221
New command: loopback-test	1221
New feature: IPS, ACG, and SSL VPN licenses	1221
New feature: Support of NQA for NETCONF	1221
New feature: Configuring CWMP to support VPN	1222
Configuring CWMP to support VPN	1222
Command reference	1222
New feature: Transceiver module source alarm	1222
Disabling transceiver module source alarm	1222
Command reference	1222
transceiver phony-alarm-disable	1222
New feature: VLAN interface performance optimization	1222
New feature: POSA	1223
POSA terminal access configuration	1223
POS terminal access command reference	1223
New feature: Specifying a backup processing slot for an interface	1223
Specifying a backup processing slot for an interface	1223
Command reference	1224
New feature: Configuring the ISDN leased line	1224
Configuring the ISDN leased line	1224
Command reference	1224
New feature: NAT support for multicast source address in PIM join/prune packets	1224
New feature: GDOI GM group anti-replay window	1225
Configuring the anti-replay window for a GDOI GM group	1225
Command reference	1225
client anti-replay window	1225

New feature: SIP compatibility	1226
Configuring SIP compatibility.....	1226
Command reference	1227
New command:sip-compatible	1227
New feature: Voice VLAN	1228
Configuring a voice VLAN.....	1228
Configuring a port to operate in automatic voice VLAN assignment mode	1228
Configuring a port to operate in manual voice VLAN assignment mode	1229
Enabling LLDP for automatic IP phone discovery	1230
Configuring LLDP to advertise a voice VLAN	1230
Configuring CDP to advertise a voice VLAN	1230
Displaying and maintaining voice VLANs	1231
Command reference	1231
New feature: L2TP-based EAD	1232
Enabling L2TP-based EAD	1232
Command reference	1232
ppp access-control enable	1232
display ppp access-control interface	1233
New feature: Configuring device poweroff alarming	1234
Command reference	1234
dying-gasp host	1234
dying-gasp source	1235
display dying-gasp host	1236
New feature: BFD for an aggregation group	1237
Enabling BFD for an aggregation group.....	1237
Command reference	1239
link-aggregation bfd ipv4.....	1239
New feature: 4G modem IMSI/SN binding authentication	1240
Command reference	1240
apn.....	1240
apn-profile.....	1241
apn-profile apply	1241
attach-format	1242
authentication-mode	1243
New feature: Media Stream Control (MSC) logging.....	1244
Command reference	1244
New command: sip log enable	1244
New feature: IMSI/SN binding authentication.....	1245
Command reference	1245
ppp lcp imsi accept.....	1245
ppp lcp imsi request.....	1246
ppp lcp imsi string.....	1246
ppp lcp sn accept	1247
ppp lcp sn request	1247
ppp lcp sn string.....	1248
ppp user accept-format imsi-sn split.....	1248
ppp user attach-format imsi-sn split.....	1249
ppp user replace	1250
New feature: Specifying a band for a 4G modem	1250
Command reference	1251
lte band	1251

New feature: Using tunnel interfaces as OpenFlow ports	1251
New feature: NETCONF support for ACL filtering	1252
Command reference	1252
netconf soap http acl	1252
netconf soap https acl	1253
New feature: WAAS	1254
Configuring WAAS	1254
Command reference	1254
New feature: Support for the MKI field in SRTP or SRTCP packets	1254
Command reference	1254
New command: mki	1254
New feature: SIP domain name	1255
Command reference	1255
New command: sip-domain	1255
New feature: E&M logging	1256
Command reference	1256
New command: em log enable	1256
New feature: Setting the RTC version	1257
Setting the RTC version	1257
Command reference	1257
rtc rtc version	1257
New feature: Setting the maximum size of advertisement files	1258
New feature: Support of IRF for NETCONF	1258
New feature: Support of VCF for NETCONF	1258
New feature: Support of SNMP for NETCONF	1258
New feature: Support of file system for NETCONF	1258
New feature: Support of PoE for NETCONF	1259
New feature: Support of RMON for NETCONF	1259
New feature: Support of policy-based routing for NETCONF	1259
New feature: Support of BGP for NETCONF	1259
New feature: Support of OSPF for NETCONF	1259
New feature: Support of ping for NETCONF	1259
New feature: Support of tracer for NETCONF	1259
New feature: Support of L2VPN for NETCONF	1260
New feature: SIP support for VRF	1260
Configuring SIP support for VRF	1260
Command reference	1260
New feature: IKEv2	1260
Configuring IKEv2	1260
Command reference	1260

New feature: Specifying an IKEv2 profile for an IPsec policy	1261
Specifying an IKEv2 profile for an IPsec policy	1261
Command reference	1261
New feature: Bidirectional BFD control detection for RIP	1261
Configuring bidirectional BFD control detection for RIP	1261
Command reference	1261
New feature: OSPF router ID autoconfiguration	1262
Automatically obtaining an OSPF router ID	1262
Command reference	1262
New feature: Layer 2 Ethernet link aggregation	1262
Configuring Layer 2 aggregation groups	1262
Command reference	1262
New feature: Setting the cable impedance for WAN interfaces	1263
Setting the cable impedance for WAN interfaces	1263
Command reference	1263
New feature: Associating a static route with a track entry	1263
Associating a static route with a track entry	1263
Command reference	1263
New feature: VLAN tag processing rule for incoming traffic	1264
Configuring the VLAN tag processing rule for incoming traffic	1264
Command reference	1264
New feature: IP-based portal-free rule	1264
Configuring an IP-based portal free-rule	1264
Command reference	1264
New feature: Portal redirect packet statistics	1265
Displaying/maintaining portal redirect packet statistics	1265
Command reference	1265
New feature: GDVPN	1265
Configuring GDVPN	1265
Command reference	1265
New feature: OpenFlow instance	1265
Configuring the OpenFlow instance mode	1265
Command reference	1266
Binding an OpenFlow instance to ports	1266
Command reference	1266
Binding a port to an OpenFlow instance	1266
Command reference	1266
New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set	1266
Enabling ESN for an IPsec transform set	1266
Command reference	1267
New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy	1267
Enabling TFC padding for an IPsec policy	1267
Command reference	1267
New feature: SIP session refresh	1267
Enabling SIP session refresh	1267

Command reference	1267
New command: voice-class sip session refresh	1267
Modified feature: License restrictions for POS terminal access	1268
Feature change description	1268
Modified feature: Displaying and maintaining Frame Relay	1269
Feature change description	1269
Command changes	1269
Modified command: display fr inarp-info	1269
Modified command: display fr lmi-info	1269
Modified command: display fr map-info	1270
Modified command: display fr pvc-info	1270
Modified feature: Displaying track entry information	1270
Feature change description	1270
Command changes	1271
Modified command: display track	1271
Modified feature: User profile	1271
Feature change description	1271
Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes	1271
Feature change description	1271
Command changes	1271
Modified command: interface tunnel	1271
Modified feature: PKI certificate auto-renewal	1272
Feature change description	1272
Command changes	1272
Modified command: certificate request mode	1272
New command: display pki certificate renew-status	1273
Modified feature: Configuring the PKI entity DN	1274
Feature change description	1274
Command changes	1275
New command: subject-dn	1275
Modified feature: ADVPN	1276
Feature change description	1276
Command changes	1276
New command: advpn group	1276
New command: advpn map group	1277
Modified feature: Telnet redirect	1278
Feature change description	1278
Modified feature: DHCP snooping performance optimization	1278
Feature change description	1278
Modified feature: OSPF performance optimization	1278
Feature change description	1278
Command changes	1279
Modified command: spf-schedule-interval	1279
Modified command: transmit-pacing	1279
Modified feature: POS terminal access	1279
Feature change description	1279
Command changes	1280
Modified command: posa auto-stop-service enable	1280

Modified feature: License	1280
Feature change description	1280
Modified feature: IP performance optimization	1280
Feature change description	1280
Command changes	1281
New command: tcp mac-record enable	1281
New command: tcp mac-record local	1281
Modified feature: AAA	1282
Feature change description	1282
Command changes	1282
New command: authorization ike	1282
Modified feature: Configuring a cellular interface for a 3G/4G modem	1283
Feature change description	1283
Command changes	1283
New command: rssi	1283
Modified feature: QoS on VXLAN tunnel interfaces	1285
Feature change description	1285
Command changes	1285
Modified feature: Option 60 encapsulation in DHCP replies	1285
Feature change description	1285
Modified feature: MPLS QoS support for matching the EXP field	1285
Feature change description	1285
Command changes	1285
New command: if-match second-mpls-exp	1285
Modified feature: MPLS QoS support for marking the EXP field	1286
Feature change description	1286
Command changes	1286
New command: remark second-mpls-exp	1286
Modified feature: Automatic configuration	1287
Feature change description	1287
Modified feature: User profile	1287
Feature change description	1287
Command change	1288
Modified command: user-profile	1288
Modified feature: Default size of the TCP receive and send buffer	1288
Feature change description	1288
Command changes	1288
Modified command: tcp window	1288
Modified feature: Obtaining fan and power module vendor information ..	1289
Feature change description	1289
Modified feature: Support for per-packet load sharing	1289
Feature change description	1289
Command changes	1289
Modified command: ip load-sharing mode	1289
Modified feature: Default user role	1290
Feature change description	1290
Command changes	1290
Modified command: role default-role enable	1290

Modified feature: Debugging	1291
Feature change description	1291
Command changes	1291
Modified command: debugging	1291
Modified feature: SSH username	1291
Feature change description	1291
Command changes	1292
Modified command: ssh user	1292
Modified feature: IS-IS hello packet sending interval	1292
Feature change description	1292
Command changes	1293
Modified command: isis timer hello	1293
Modified feature: MP-group interface numbering	1293
Modified feature: Setting the global link-aggregation load-sharing mode ..	1293
Feature change description	1293
Command changes	1293
Modified command: link-aggregation global load-sharing mode	1293
Modified feature: 802.1X redirect URL	1294
Feature change description	1294
Command changes	1294
Modified command: dot1x ead-assistant url	1294
Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server	1295
Feature change description	1295
Command changes	1295
Modified command: display ntp-service trace	1295
Modified feature: Saving, rolling back, and loading the configuration	1295
Modified feature: Displaying information about SSH users	1296
Feature change description	1296
Command changes	1296
Modified command: display ssh user-information	1296
Modified feature: SIP trusted nodes	1296
Configuring SIP trusted nodes	1296
Command changes	1296
New command: display voice ip address trusted list	1297
New command: ip address trusted authenticate	1298
Modified feature: IPsec ESP encryption algorithms	1298
Feature change description	1298
Command changes	1299
Modified feature: IPsec ESP authentication algorithms	1299
Feature change description	1299
Command changes	1300
Modified feature: IPsec AH authentication algorithms	1300
Feature change description	1300
Command changes	1300
Modified feature: Specifying an encryption algorithm for an IKE proposal	1301
Feature change description	1301

Command changes	1301
Modified feature: Specifying an authentication algorithm for an IKE proposal	
.....	1302
Feature change description	1302
Command changes	1302
Modified feature: Generating asymmetric key pairs	1302
Feature change description	1302
Command changes	1302
Modified feature: Specifying an ECDSA key pair for certificate request ...	1303
Feature change description	1303
Command changes	1303
Modified feature: Setting the electrical impedance	1303
Feature change description	1303
Command changes	1303
Modified feature: POS access statistics, SNMP notifications for POS access, and NII	1304
Feature change description	1304
Enabling SNMP notifications for POS access	1304
Configuring the alarm threshold for the low NII transaction success rate	1304
POS terminal packet statistics based on E1POS interfaces	1304
Displaying and maintaining terminal access	1304
Command changes	1304
Modified command: snmp-agent trap enable posa	1304
New command: trade-exchanges	1305
New command: posa trade-falling-threshold	1305
New command: posa e1-dial-falling-threshold	1305
New command: display posa statistics caller-id	1305
New command: display posa statistics caller-ip	1305
New command: display posa statistics nii	1305
Modified command: reset posa statistics	1305
Modified feature: QoS MIB	1306
Feature change description	1306
Modified feature: Enabling PFS for an IPsec transform set	1306
Feature change description	1306
Command changes	1306
Removed feature: Tiny proxy	1306
Feature change description	1306
Removed command	1306
http-proxy	1306
Removed feature: Displaying switching fabric channel usage	1307
Feature change description	1307
Removed command	1307
display fabric utilization	1307
Release 0304	1307
New feature: Setting the RTC version	1308
Configuring Setting the RTC version	1308
Command reference	1308
rtc rtc version	1308

New feature: Setting the maximum size of advertisement files	1309
Configuring the maximum size of advertisement files	1309
Command reference	1309
New feature: IRF	1309
Configuring IRF	1309
Command reference	1310
New feature: Frame Relay	1310
Configuring Frame Relay	1310
Command reference	1310
New feature: EVI	1310
Configuring EVI	1310
Command reference	1310
New feature: VPLS	1310
Configuring VPLS	1310
Command reference	1310
New feature: Multicast VPN support for inter-AS option B	1311
Configuring Multicast VPN support for inter-AS option B	1311
Command reference	1311
Modified feature: 802.1X redirect URL	1311
Feature change description	1311
Command changes	1311
Modified command: dot1x ead-assistant url	1311
Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server	1312
Feature change description	1312
Command changes	1312
Modified command: display ntp-service trace	1312
Modified feature: Saving, rolling back, and loading the configuration	1312
Feature change description	1312
Command changes	1313
Modified feature: Displaying information about SSH users	1313
Feature change description	1313
Command changes	1313
Modified command: display ssh user-information	1313
Removed feature: Displaying fabric utilization	1313
Feature change description	1313
Removed command	1314
display fabric utilization	1314
ESS 0302P06	1314
New feature: Object policies	1315
Configuring Object policies	1315
Command reference	1315
New feature: IPHC	1315
Configuring IPHC	1315
Command reference	1315

New feature: Support of PPPoE server for IPv6	1315
Configuring Support of PPPoE server for IPv6	1315
Command reference	1316
New feature: QSIG tunneling over SIP-T	1316
Configuring QSIG tunneling over SIP-T	1316
Command reference	1316
New feature: Playout delay	1316
Configuring Playout delay	1316
Command reference	1316
New feature: BGP L2VPN support for NSR	1316
Configuring BGP L2VPN support for NSR	1316
Command reference	1317
New feature: BGP support for dynamic peers	1317
Configuring BGP support for dynamic peers	1317
Command reference	1317
New feature: ARP PnP	1317
Configuring ARP PnP	1317
Command reference	1317
New feature: Support of Syslog for DNS and support of customlog&userlog for IPv6 hosts	1318
Configuring Support of Syslog for DNS and support of customlog&userlog for IPv6 hosts	1318
Command reference	1318
New feature: QoS soft forwarding	1318
Configuring QoS soft forwarding	1318
Command reference	1319
New feature: Filtering by application layer protocol status	1319
Configuring Filtering by application layer protocol status	1319
Command reference	1319
New feature: ADVPN support for multicast forwarding	1319
Configuring ADVPN support for multicast forwarding	1319
Command reference	1319
New feature: MPLS LDP support for IPv6	1320
Configuring MPLS LDP support for IPv6	1320
Command reference	1320
New feature: Port security	1320
Configuring Port security	1320
Command reference	1321
New feature: Customizable IVR	1321
Configuring Customizable IVR	1321
Command reference	1321
New feature: SRST	1321
Configuring SRST	1321
Command reference	1321
New feature: NEMO	1322
Configuring NEMO	1322
Command reference	1322

New feature: Support of MFR and FR for L2VPN, FR QoS, and FR compression and fragmentation	1322
Configuring Support of MFR and FR for L2VPN, FR QoS, and FR compression and fragmentation	1322
Command reference	1322
New feature: Support for LLDP on CPOS interfaces	1323
Configuring Support for LLDP on CPOS interfaces	1323
Command reference	1323
New feature: SMS-based automatic configuration	1323
Configuring SMS-based automatic configuration	1323
Command reference	1323
New feature: ARP attack protection	1323
Configuring ARP attack protection	1323
Command reference	1324
New feature: SIP support for VRF	1324
Configuring SIP support for VRF	1324
Configuration guidelines	1324
Configuration procedure	1324
Command reference	1324
vpn-instance	1324
ESS 0102	1325
New feature: Portal authentication	1326
Command reference	1326
New feature: MSDP	1326
Configuring MSDP	1326
Command reference	1327
New feature: IPsec MIB and IKE MIB	1327
New feature: PoE	1327
Configuring PoE	1327
Command reference	1328
New feature: CoPP software forwarding feature	1328
Configuring CoPP	1328
Command reference	1328
control-plane	1328
control-plane management	1329
qos apply policy (interface view, control plane view)	1329
New feature: Configuring MPLS LDP FRR	1331
Configuring MPLS LDP FRR	1331
Command reference	1331
igp sync delay	1331
igp sync delay on-restart	1333
mpls ldp igp sync disable	1334
New feature: Enhanced routing features	1334
Configuring enhanced routing features	1334
Command reference	1335
non-stop-routing	1335
ip route-static fast-reroute auto	1335
import-route (RIP view)	1336
import-route (OSPF view)	1337

import-route (IS-IS view)	1339
import-route (BGP view)	1341
import-route (RIPng view)	1343
import-route (OSPFv3 view)	1344
ipv6 import-route (IPv6 IS-IS view)	1346
New feature: Python	1347
Using Python	1347
Command reference	1348
New feature: ATM	1348
Configuring ATM	1348
Command reference	1348
New feature: DHCP MIB	1348
DHCP MIB	1348
Command reference	1348
if-match	1348
ESS 0006P02	1350

Release 6749P14

This release has the following changes:

New feature: Link flapping protection on an interface

New feature: SRv6 and MPLS interworking

New feature: Applying a QoS policy to an SRv6 TE policy

New feature: SRv6 service chain

New feature: Configuring 8-queue PQ

New feature: Configuring an SDWAN TTE information match criterion and a VPN instance match criterion

New feature: Simplifying the QoS configuration in a hub-spoke network

New feature: Configuring interface channelization

New feature: Configuring a default color value for public network and L3VPN route recursion to an SRv6 TE policy

New feature: SRv6 TE policy route recursion support for SRv6-TE and SRv6-BE FRR mode

New feature: Configuring the SRv6 TE policy encapsulation mode

New feature: Configuring the Next Header field value in the SRH of SRv6 packets

New feature: SRv6 TE policy rate limit

New feature: Configuring next hop-based dynamic End.DX4 or End.DX6 SID allocation for public or private network routes

New feature: VPNv4/VPNv6/EVPN routes

New feature: G-SRv6

New feature: Configuring the SRv6 MTU

New feature: Configuring the SRv6 DiffServ mode

New feature: BGP-EPE

New feature: SRv6 TE Policy CBTS

New feature: Enabling the device to distribute SRv6 TE policy candidate path information to BGP-LS

New feature: SRv6 TE policy egress protection

New feature: Enabling the device to drop traffic when an SRv6 TE policy becomes invalid

New feature: Automatic route advertisement for an SRv6 TE policy

New feature: EVPN VPLS over SRv6/EVPN VPWS over SRv6

New feature: Configuring IPv6 Flowspec

New feature: MP packet fast forwarding

New feature: Setting the traffic statistics update timer for IPoE sessions

New feature: Configuring the time interval for traffic rate calculation of portal users

New feature: Disabling sending a specific type of ICMP messages

New feature: Disabling receiving a specific type of ICMP messages

New feature: Display the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state

New feature: Python2 progress monitoring

New feature: Software upgrade through CWMP
New feature: Specifying a CPE service port number
New feature: Configuring the notification format and enabling notifications to carry the device serial number (SN)
New feature: Configuring SQANew feature: Specifying the number of CPU cores allocated as control cores
New feature: Enabling the capability of MPLS BFD to trigger tunnel-down

New feature: Configuring resource monitoring

New feature: Tunnel BFD for LSPs

New feature: Tunnel BFD for MPLSTE tunnels

New feature: Configuring the rule for adding BGP routes to the IP routing table and the route advertisement rule for VPN instances

New feature: Specifying an MPLS label allocation mode

New feature: Setting an MPLS label range for all VPN instances

New feature: Applying the export routing policy to VPNv4 routes before RT filtering

New feature: Configuring a BJCA authentication server

New feature: Enabling transparent transmission of LLDP frames

New feature: Transparent LACPDU transmission

New feature: Configuring VLAN mapping

New feature: PKI domain for communication with a JIT authentication server

New feature: SDWAN

New feature: STUN

New feature: Specifying a CWMP NTP server

New feature: Enabling route advertisement for IPv6 prefixes assigned to directly connected clients

New feature: Enabling the DHCPv6 relay agent to support Option 79

New feature: mGRE NHS and NHRP packet sending related features

New feature: Setting the length of called numbers when R2 signaling is used to access the POS terminal

New feature: Establishing an MQTT connection

New feature: Configuring packet duplication optimization parameters

New feature: Setting the reorder timeout timer for load balancing packets

New feature: Configuring TCP MSS automatic adjustment

New feature: Configuring BGP GR

New feature: Support for filtering routes by the Priority-Color extended community attribute

New feature: Configuring automatic SIM registration

New feature: Configuring TCP congestion control algorithm for TCP proxy

New feature: Specifying the longest match principle for next hop recursion

New feature: Configuring POS application load sharing and FEP group backup

New feature: Disabling BGP from flushing specific routes to the routing table

New feature: Configuring the POS application connection keep feature

New feature: RIR-SDWAN

New feature: SaaS path optimization

New feature: Specifying a VXLAN tunnel as a dedicated link for a flow template

New feature: Enabling the device to drop service flows upon failure to find an optimal link

New feature: Configuring FEC optimization parameters

New feature: Specifying the 5G NR network mode for the 5G modem to register with

New feature: Configuring TCP packet compression or decompression

New feature: Preferring routes learned from a peer or peer group during optimal route selection

New feature: Configuring the BGP Additional Paths feature

New feature: Allowing the RR to change the attributes of routes to be reflected

New feature: Configuring packet duplication optimization

New feature: Specify an ACL to match the TCP or UDP packets that can be compressed or decompressed

New feature: Configuring packet duplication parameters

New feature: Setting the reorder timeout timer for load balancing packets

New feature: Support for the link tag feature

Modified feature: Binding a POS terminal template to an interface and configuring a POS application mapping entry

Modified feature: Configuring RIR in RIR-SDWAN view, RIR-SDWAN flow template view, and RIR-SDWAN SLA view

Modified feature: Displaying unicast routing information generated based on the Priority-Color extended community attribute

Modified feature: Specifying a TCP congestion control algorithm for the WAN side

Modified feature: RIR support for VPDN links

Modified feature: Using the original cost of redistributed routes

Modified feature: Configuring IS-IS to redistribute user network routes and redistribute routes without keeping their SR labels

Modified feature: Setting the speed of an Ethernet interface

Modified feature: Configuring load sharing for link aggregation groups based on flow labels

Modified feature: QinQ support for new views and keywords

Modified feature: QinQ support for new keywords

Modified feature: Recursing an IPv6 static route to the specified SRv6 TE policy

Modified feature: Recursing a static route to the specified SRv6 TE policy

Modified feature: Support for specifying a BJCA server for an AAA private-protocol scheme

Modified feature: Support of configuring an AAA private protocol scheme for IKE extended authentication

Modified feature: Support of displaying IPv4 unicast routing information generated based on the Priority-Color extended community attribute for a BGP-VPN instance routing table

Modified feature: Configuring the parameters carried in the URL of a portal Web server

Modified feature: Change of default values for the single-hop BFD detection time multiplier and SBFD detection time multiplier

Modified feature: Displaying VRRP version information in the output from the display vrrp command

Modified feature: Configuring the parameters carried in the URL of a portal Web server

Modified feature: Using the gateway IP address obtained from the DHCP server through the specified interface as the next hop IP address for probe packets

Modified feature: Specifying the aging parameters for dynamic flows

Modified feature: Specifying the measurement period for an iFIT instance

Modified feature: Binding additional analyzers to a collector instance

Modified feature: Binding an MP to an interface

Modified feature: Specifying the length of probe packets for a tracer operation

Modified feature: Specifying the source IPv6 address of the probe packets for an IPv6 tracer operation

Modified feature: Setting the flow log versionModified feature: Filtering the output from a display command with a regular expression

Modified feature: Configuring the NAT device to ignore the protocol packet type

Modified feature: Static port blocks for AFT

New feature: Support of URL-based automatic configuration for encryption

New feature: Support of USB-based automatic configuration for encryption

New feature: Configuring DNS redirection

New feature: Enabling DNS server health check

New feature: Disabling receiving a specific type of ICMPv6 messages

New feature: Disabling sending a specific type of ICMPv6 messages

New feature: Enabling advertising invalid delegated prefixes

New feature: Setting the TTL value for DNS entries

New feature: Configuring DNS filtering

New feature: Configuring DNS snooping

New feature: Configuring the DNS transparent proxy

Modified feature: Displaying the running configuration

Modified feature: Displaying the contents of the configuration file for the next system startup

Modified feature: Displaying the running configuration in the current view

Modified feature: Configuring an ACL match criterion

Modified feature: Adding a node to a SID list

Modified feature: Configuring a traffic redirection action

Modified feature: Clearing forwarding statistics for all SRv6 TE policies

Modified feature: Enabling Router ID filtering

Modified feature: Support of the ipv6 route-static command for the gateway keyword

New feature: License installation and AC configuration

New feature: Configuring bandwidth guaranteeing

New feature: Enabling NetStream sampling for an SRv6 TE policy

New feature: Enabling NetStream for an SRv6 TE policy

New feature: Enabling IPv6 NetStream sampling for an SRv6 TE policy

New feature: Enabling IPv6 NetStream for an SRv6 TE policy

New feature: Importing the carrier address library at the GUI

New feature: Configuring the time zone at the GUI

New feature: Enabling Web logging

Modified feature: Specifying multiple NTP servers

Modified feature: Flow-mirroring traffic to an interface

New feature: EoGRE

New feature: Configuring ARP attack detection on the Web interface

New feature: Configuring NAT address pools on the Web interface

New feature: Configuring application services on the Web interface

New feature: Configuring a PCE

New feature: Configuring stateful PCE on a PCC

New feature: Configuring PCEP session parameters

New feature: Displaying local PCEP session settings and stateful PCE peers information

Modified feature: Configuring a NAT port mapping

Modified feature: Enabling BFD for LSPs associated with an FEC

Modified feature: Displaying LSP information

Modified feature: Configuring a preferred tunnel in a tunnel policy

Modified feature: Binding tunnels to a destination IP address in a tunnel policy

New feature: Reserving an MPLS TE tunnel for tunnel binding policies

Modified feature: Configuring one-to-one mappings on the Web interface

Modified feature: Support of configuring Option 82 on a VEB interface

Modified feature: Configuring a private address-to-public address mapping for an NHS of mGRE

Modified feature: Support for configuring Web Cache for devices in the RIR-SDWAN scenario

New feature: Configuring optimized features for HTTP proxy

New feature: Configuring HTTP proxy in an HTTP proxy server view

New feature: Support for proxy NTLM authentication packets and obtaining the suffix of a Web cache file from the PMO website URL

New feature: Enhancing tunnel maintenance

New feature: Configuring dual-device backup for Web caching

New feature: Enabling HTTPS-based Web caching

New feature: ADVPN support specifying the link protocol type of the hub

New feature: GRE keepalive support for the reply-check-only mode

New feature: eMDI

New feature: Enabling SNMP notifications for OpenFlow

New feature: EVPN VPLS

New feature: EVPN VPWS

New feature: EVPN VXLAN forwarding mode

New feature: Enabling an ED to replace the L3 VXLAN ID, RD, and route targets of BGP EVPN routes

New feature: Enabling EVPN to advertise VPN routes

Modified feature: Displaying BGP EVPN route information with the specified prefix

Modified feature: Saving the configuration in safe mode

New feature: Configuring MACsec

New feature: Configuring the device as responder-only for IPsec SA negotiation

New feature: Specifying a security enhanced level

New feature: Configuring GD-quantum encryption

New feature: Enabling SNMP notifications for PKI

New feature: Configuring the initiator to use dynamic source UDP ports for IKE negotiations

New feature: Binding a smart token to the device

New feature: Configuring the title for the PKI entity

New feature: Configuring ZD-quantum encryption

New feature: Setting a limit to the number of IKEv2 SAs

Modified feature: Displaying information about IPsec SAs

Modified feature: Configuring a peer ID for IKE profile matching

Modified feature: Configuring a preshared key

Modified feature: Enabling ALG to process IP fragments and TCP segments

Modified feature: Not support for DES, 3DES, MD5, RC4, and RC2 cipher suites in SSL client and server policies

Modified feature: Not support for an SSL protocol version lower than TLS 1.1 for session negotiation

Modified feature: Disabling SSL session renegotiation

Modified feature: Displaying information about SDWAN IPsec tunnels

Modified feature: Specifying the user information required for client authentication

Modified feature: Displaying information about IKE SAs

Modified feature: Displaying IKE statistics

Modified feature: Displaying the IKEv2 SA information

Modified feature: Displaying IKEv2 statistics

Modified feature: Support for the incremental increase in user locking period

New feature: Link flapping protection on an interface

Enabling link flapping protection on an interface

About this task

Link flapping on an interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when interface status on the active link changes between **UP** and **DOWN**, traffic switches between active and standby links. To solve this problem, configure this feature on the interface.

With this feature enabled on an interface, when the interface goes down, the system enables link flapping detection. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Restrictions and guidelines

This feature takes effect only if it is configured in both the system view and interface view.

IRF system stability might be affected by IRF physical link flapping. For IRF system stability, this feature is enabled by default on IRF physical interfaces and the enabling status of this feature is not affected by the status of global link flapping protection. When the number of flaps detected on an IRF physical interface exceeds the threshold within the detection interval, the device outputs a log rather than shuts down the IRF physical interface.

The **dampening**, **link-delay**, and **port link-flap protect enable** commands are mutually exclusive on an Ethernet interface.

To bring up an interface that has been shut down by link flapping protection, execute the **undo shutdown** command.

In the **display interface** command output, the **Link-Flap DOWN** value of the **Current state** field indicates that the interface has been shut down by link flapping protection.

Procedure

1. Enter system view.
system-view
2. Enable link flapping protection globally.
link-flap protect enable
By default, link flapping protection is disabled globally.
3. Enter Ethernet interface view.
interface *interface-type* *interface-number*
4. Enable link flapping protection on the Ethernet interface.
port link-flap protect enable [**interval** *interval* | **threshold** *threshold*] *
By default, link flapping protection is disabled on an Ethernet interface.

Display and maintenance commands for Ethernet interfaces

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information about link flapping protection on interfaces.	display link-flap protection [interface <i>interface-type</i> [<i>interface-number</i>]]
Display the physical link state change statistics of interfaces.	display link-state-change statistics interface [<i>interface-type</i> [<i>interface-number</i>]]
Clear the physical link state change statistics of interfaces.	reset link-state-change statistics interface [<i>interface-type</i> [<i>interface-number</i>]]

Command reference

New command: display link-flap protection

Use **display link-flap protection** to display information about link flapping protection on an interface.

Syntax

display link-flap protection [**interface** *interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface *interface-type* [*interface-number*] : displays information about link flapping protection on an interface. The *interface-type* parameter specifies an interface type. The *interface-number* parameter specifies an interface number. If you do not specify an interface type, the command displays information about link flapping protection on all interfaces.

Usage guidelines

If you do not specify an interface number, the command displays information about link flapping protection on all interfaces of the specified type.

Examples

Display information about link flapping protection on all interfaces.

```
<Sysname> display link-flap protection
Link-flap protection: Enabled
Interface          Link-flap  Status  Interval  Threshold
GE1/0/1            Enabled    Down    10         5
GE1/0/2            Disabled   N/A     --         --
```

Table 1 Command output

Field	Description
Link-flap protection	Status of global link flapping protection: • Enabled—Link flapping protection is enabled globally. • Disabled—Link flapping protection is disabled globally.
Link-flap	Status of link flapping protection on an interface: • Enabled—Link flapping protection is enabled on an interface. • Disabled—Link flapping protection is disabled on an interface.
Status	Status of an interface: • Down—The interface has been shut down by the link flapping protection feature. • N/A—The interface status is not affected by the link flapping protection feature.
Interval	Link flapping detection interval for an interface.
Threshold	Link flapping detection threshold for an interface.

Related commands

link-flap protect enable
port link-flap protect enable

New command: display link-state-change statistics interface

Use **display link-state-change statistics interface** to display the link state change statistics of interfaces.

Syntax

display link-state-change statistics interface [*interface-type* [*interface-number*]]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-type: Specifies an interface type.
interface-number: Specifies an interface number.

Usage guidelines

If you do not specify an interface type and an interface number, this command displays the link state change statistics for all up interfaces that have traffic counters.

If you specify an interface type but do not specify an interface number, this command displays the link state change statistics for all interfaces of the specified type.

Examples

Display the link state change statistics for all interfaces.

```
<Sysname> display link-state-change statistics interface
```

Interface	Change-times	Last-change-time	Reset link-state time
		Link-flap-begin	Link-flap-end
GE1/0/1	0	Never	Never
		Never	Never

Table 2 Command output

Field	Description
Interface	Abbreviated interface name.
Change-times	Number of physical state changes.
Last-change-time	Last time when the physical state changed.
Reset link-state time	Time when the link state change statistics were cleared.
Link-flap-begin	Last time when a link state flapping began. If no link state flapping has occurred, this field displays Never .
Link-flap-end	Last time when a link state flapping ended. If no link state flapping has occurred, this field displays Never .

Related commands

reset link-state-change statistics interface

New command: link-flap protect enable

Use **link-flap protect enable** to enable link flapping protection globally.

Use **undo link-flap protect enable** to disable link flapping protection globally.

Syntax

link-flap protect enable

undo link-flap protect enable

Default

Link flapping protection is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Link flapping on any interface changes network topology and increases the system overhead. For example, in an active/standby link scenario, when the interface status on the active link changes between **UP** and **DOWN**, traffic switches between active and standby links. To solve this problem, execute this command.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

Link flapping protection takes effect only when it is enabled in both system view and interface view.

Examples

```
# Enable link flapping protection globally.
```

```
<Sysname> system-view
```

```
[Sysname] link-flap protect enable
```

Related commands

port link-flap protect enable

New command: port link-flap protect enable

Use **port link-flap protect enable** to enable link flapping protection on an interface.

Use **undo port link-flap protect enable** to disable link flapping protection on an interface.

Syntax

port link-flap protect enable [*interval interval* | *threshold threshold*] *

undo port link-flap protect enable [*interval* | *threshold*]

Default

Link flapping protection is disabled on an interface.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

interval interval: Specifies the link flapping detection interval in seconds. The value range for this argument is 10 to 60. The default value for this argument is 10.

threshold threshold: Specifies the link flapping detection threshold in the range of 5 to 10. The default value for this argument is 5.

Usage guidelines

Link flapping protection takes effect only when it is enabled in both system view and interface view.

If you do not specify the **interval** *interval* or **threshold** *threshold* option when you execute the **port link-flap protect enable** command, the command uses the default settings.

If you specify the **interval** or **threshold** keyword when you execute the **undo port link-flap protect enable** command, the command restores the default setting for the keyword.

With link flapping protection enabled on an interface, when the interface goes down, the system enables link flapping detection on the interface. During the link flapping detection interval, if the number of detected flaps reaches or exceeds the link flapping detection threshold, the system shuts down the interface.

To bring up an interface that has been shut down by link flapping protection, execute the **undo shutdown** command.

This command, the **dampening** command, and the **link-delay** command are mutually exclusive on an Ethernet interface.

Examples

Enable link flapping protection on an interface. Set the link flapping detection interval to 10 seconds, and set the link flapping detection threshold to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-flap protect enable interval 10 threshold 5
```

Related commands

dampening

link-delay

link-flap protect enable

New command: reset link-state-change statistics interface

Use **reset link-state-change statistics interface** to clear link state change statistics of interfaces.

Syntax

reset link-state-change statistics interface [*interface-type* [*interface-number*]]

Default

Link state change statistics of an interface are not cleared.

Views

User view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

Usage guidelines

If you do not specify an interface type, this command clears the link state change statistics for all interfaces.

If you specify an interface type but do not specify an interface number, this command clears the link state change statistics for all interfaces of the specified type.

Examples

Clear the link state change statistics of Ten-GigabitEthernet 1/0/1.

```
<Sysname> reset link-state-change statistics interface ten-gigabitethernet 1/0/1
```

Related commands

display link-state-change statistics interface

New feature: SRv6 and MPLS interworking

Configuring SRv6 and MPLS interworking

Configuring inter-AS option B VPN

About this task

For intercommunication between an MPLS network in one AS and an SRv6 network in another AS, enable SRv6 and MPLS interworking on the ASBR in the SRv6 network. This feature enables End.T SID allocation and establishes mappings between End.T SIDs and MPLS labels.

Restrictions and guidelines

After you enable SRv6 and MPLS interworking, the per-next-hop label allocation mode applies to routes forwarded from SRv6 networks to MPLS networks. The label allocation mode is not affected by the **label-allocation-mode** or **apply-label** command. For more information about the **label-allocation-mode** command, see BGP commands in *Layer 3—IP Routing Command Reference*. For more information about the **apply-label** command, see MPLS L3VPN commands in *MPLS Command Reference*.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP EVPN address family view.
address-family l2vpn evpn
4. Enable the device to reoriginate BGP EVPN routes based on the BGP EVPN routes received from a peer or peer group.
peer { group-name | ipv4-address [mask-length] | ipv6-address [prefix-length] } re-originated [replace-rt]
By default, the device does not reoriginate BGP EVPN routes based on received BGP EVPN routes.
5. (Optional.) Enable the device to advertise original BGP EVPN routes to a peer or peer group.
peer { group-name | ipv4-address [mask-length] | ipv6-address [prefix-length] } advertise original-route

By default, the device advertises only reoriginated BGP EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

6. (Optional.) Suppress advertisement of reoriginated BGP EVPN routes to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
suppress re-originated ip-prefix

By default, the device advertises reoriginated BGP EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

7. Enable SRv6 and MPLS interworking.

srv6-mpls-interworking enable

By default, SRv6 and MPLS interworking is disabled.

8. Apply a locator to the BGP VPN instance.

segment-routing ipv6 locator *locator-name evpn* [**auto-sid-disable**]

By default, no locator is applied to a BGP VPN instance.

9. Configure the route recursion mode.

segment-routing ipv6 { **best-effort** | **traffic-engineer** | **traffic-engineer best-effort** }
evpn

By default, a PE searches the IPv6 routing table based on the next hop of a matching route to forward traffic.

Configuring optimal route reorigination and advertisement

About this task

Configure this feature on an MPE that connects the MPLS L3VPN and MPLS L3VPN over SRv6 networks. This feature enables the MPE to reoriginate the optimal BGP VPNv4 or VPNv6 routes for intercommunication between the MPLS and SRv6 networks.

With this feature, the MPE performs the following operations after receiving BGP VPNv4 or VPNv6 routes:

1. Matches the route targets of the routes with the import route targets of local VPN instances.
2. Reoriginates the optimal routes in the matching VPN instance. The optimal routes include the private network label or an SRv6 SID.
3. Advertises the reoriginated routes to VPNv4 or VPNv6 peers.

The reoriginated routes include the RD of the VPN instance. In addition, the route targets of the VPN instance are added to the routes based on the original routes.

Restrictions and guidelines

Configure all settings in this section on an MPE.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP-VPN instance view.
ip vpn-instance *vpn-instance-name*

4. Enter BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view.
 - o Enter BGP-VPN IPv4 unicast address family view.
address-family ipv4 [unicast]
 - o Enter BGP-VPN IPv6 unicast address family view.
address-family ipv6 [unicast]
5. Configure the device to reoriginate the optimal routes in the VPN instance and advertise the reoriginated routes to VPNv4 or VPNv6 peers.
advertise route-reoriginate
 By default, the device does not reoriginate the optimal routes in a VPN instance. The original VPNv4 or VPNv6 routes are advertised to VPNv4 or VPNv6 peers.

SRv6 and MPLS interworking

srv6-mpls-interworking enable

Use **srv6-mpls-interworking enable** to enable SRv6 and MPLS interworking.

Use **undo srv6-mpls-interworking enable** to disable SRv6 and MPLS interworking.

Syntax

srv6-mpls-interworking enable

undo srv6-mpls-interworking enable

Default

SRv6 and MPLS interworking is disabled.

Views

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Predefined user roles

network-admin

Usage guidelines

For intercommunication between an MPLS network in one AS and an SRv6 network in another AS, enable SRv6 and MPLS interworking on the ASBR in the SRv6 network. This feature enables End.T SID allocation and establishes mappings between End.T SIDs and MPLS labels.

With this feature, the ASBR in the SRv6 network allocates End.T SIDs based on FECs and advertises the SIDs to other SRv6 nodes through an IGP. An FEC is a destination IPv4 address/mask or destination IPv6 address/prefix length. The function of an End.T SID is removing the outer IPv6 header and looking up the IPv6 FIB table based on the End.T SID to forward packets.

For SRv6-to MPLS packets, the ingress node in the SRv6 network encapsulates an End.T SID to the packets when forwarding the packets to the ASBR in the SRv6 network. When the ASBR in the SRv6 network receives the packets, it looks up the IPv6 FIB table based on the End.T SID for a matching route. Then, the ASBR recurses the route to an LSP to forward the packets to the MPLS network.

For MPLS-to-SRv6 packets, the ASBR in the SRv6 network looks up the label forwarding table to forward the packets. The out label is an End.DT4, End.DT6, End.DT46, End.DX4, or End.DX6 SID in the SRv6 network. After the ASBR in the SRv6 network encapsulates the End.DT4, End.DT6,

End.DT46, End.DX4, or End.DX6 SID to the packets, it forwards the packets in SRv6-BE or SRv6-TE mode.

Examples

Enable SRv6 and MPLS interworking.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family vpnv4
[Sysname-bgp-default-vpnv4] srv6-mpls-interworking enable
```

advertise route-reoriginate

Use **advertise route-reoriginate** to reoriginate the optimal routes in a VPN instance and advertise the reoriginated routes to VPNv4 or VPNv6 peers.

Use **undo advertise route-reoriginate** to restore the default.

Syntax

advertise route-reoriginate

undo advertise route-reoriginate

Default

The device does not reoriginate the optimal routes in a VPN instance. The original VPNv4 or VPNv6 routes are advertised to VPNv4 or VPNv6 peers.

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

All settings in this section are configured on an MPE.

In the HoVPN scenario, UPEs can reach each other through an MPE and SPE. If the network has a large number of UPEs, the SPE will receive abundant UPE routes that include labels from the MPE. Forwarding failure might occur for UPEs if the SPE does not have sufficient routing entry resources to store the UPE routes.

To reduce the number of routes advertised to the SPE, use this command on the MPE. When the MPE receives VPNv4 or VPNv6 routes, it compares the export targets of the routes with the local import route targets of the corresponding VPN instance. If the route targets match, the device reoriginates the optimal routes in the VPN instance and advertises the reoriginated routes to VPNv4 or VPNv6 peers.

The reoriginated routes include the RD of the VPN instance. In addition, the route targets of the VPN instance are added to the routes based on the original routes.

Examples

In BGP-VPN IPv4 unicast address family view, configure the device to reoriginate the optimal routes in VPN instance **vpn1** and advertise the reoriginated routes to VPNv4 peers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpn1
[Sysname-bgp-default-vpn1] address-family ipv4
```

[Sysname-bgp-default-ipv4-vpn1] advertise route-reoriginate

Modified command: segment-routing ipv6 best-effort

Use **segment-routing ipv6 best-effort** to recurse routes to SRv6-BE tunnels.

Use **undo segment-routing ipv6 best-effort** to restore the default.

Old syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 best-effort [evpn]

undo segment-routing ipv6 best-effort [evpn]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 best-effort

undo segment-routing ipv6 best-effort

New syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 best-effort [evpn]

undo segment-routing ipv6 best-effort [evpn]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 best-effort

undo segment-routing ipv6 best-effort

In BGP EVPN address family view:

segment-routing ipv6 best-effort evpn

undo segment-routing ipv6 best-effort evpn

In BGP IPv4 unicast address family view or BGP IPv6 unicast address family view:

segment-routing ipv6 best-effort

undo segment-routing ipv6 best-effort

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Change description

This feature was added in BGP VPNv4 address family view, BGP VPNv6 address family view, and BGP EVPN address family view. This feature is applicable to the inter-AS option B VPN scenario.

Modified command: segment-routing ipv6 locator

Use **segment-routing ipv6 locator** to add the SID attribute to private network routes when the routes are converted to BGP VPNv4, VPNv6, IPv4 unicast, IPv6 unicast, or EVPN routes.

Use **undo segment-routing ipv6 locator** to restore the default.

Old syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 locator *locator-name* [**evpn**] [**auto-sid-disable**]

undo segment-routing ipv6 locator [**evpn**]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 locator *locator-name* [**auto-sid-disable**]

undo segment-routing ipv6 locator

New syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 locator *locator-name* [**evpn**] [**auto-sid-disable**]

undo segment-routing ipv6 locator [**evpn**]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 locator *locator-name* [**auto-sid-disable**]

undo segment-routing ipv6 locator

In BGP EVPN address family view:

segment-routing ipv6 locator *locator-name* **evpn** [**auto-sid-disable**]

undo segment-routing ipv6 locator evpn

In BGP IPv4 unicast address family view or BGP IPv6 unicast address family view:

segment-routing ipv6 locator *locator-name* [**auto-sid-disable**]

undo segment-routing ipv6 locator

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Change description

This feature was added in BGP VPNv4 address family view, BGP VPNv6 address family view, and BGP EVPN address family view.

Modified command: segment-routing ipv6 traffic-engineering

Use **segment-routing ipv6 traffic-engineering** to recurse routes to SRv6 TE policy tunnels.

Use **undo segment-routing ipv6 traffic-engineering** to restore the default.

Old syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**] [**evpn**]

undo segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**] [**evpn**]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 traffic-engineering [**best-effort**]

undo segment-routing ipv6 traffic-engineering [**best-effort**]

New syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**] [**evpn**]

undo segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**] [**evpn**]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 traffic-engineering [**best-effort**]

undo segment-routing ipv6 traffic-engineering [**best-effort**]

In BGP EVPN address family view:

segment-routing ipv6 traffic-engineering [**best-effort**] **evpn**

undo segment-routing ipv6 traffic-engineering [**best-effort**] **evpn**

In BGP IPv4 unicast address family view or BGP IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**]

undo segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**]

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Change description

This feature was added in BGP VPNv4 address family view, BGP VPNv6 address family view, and BGP EVPN address family view. This feature is applicable to the inter-AS option B VPN scenario.

New feature: Applying a QoS policy to an SRv6 TE policy

Applying the QoS policy to an SRv6 TE policy

About this task

In an L3VPN over SRv6 TE policy, you need to classify packets by VPN on the ingress of an SRv6 TE policy and then take QoS actions on matching packets, for example, traffic shaping. You can also perform QoS scheduling based on the 5-tuple of original packets of the same VPN. Applying a QoS policy to the output interface on the ingress of an SRv6 TE policy can only match the outer header information of SRv6-encapsulated packets instead of the original packet header information. This task can solve the problem.

With this function configured, the device applies the specified QoS policy to all original packets steered to an SRv6 TE policy and perform SRv6 encapsulation and forwarding on the original packets according to the SRv6 TE policy. For more information SRv6 TE policy, see *Segment Routing Configuration Guide*.

Restrictions and guidelines

This function takes effect only on the ingress of an SRv6 TE policy.

Only one QoS policy can be applied to an SRv6 TE policy. To apply a new QoS policy to an SRv6 TE policy that has one QoS policy applied, first execute the **undo qos apply policy srv6-policy** command.

Procedure

1. Enter system view.
system-view
2. Apply the QoS policy to the SRv6 TE policy.
qos apply policy *policy-name* **srv6-policy end-point ipv6** *ipv6-address* **color** *color-value* **outbound**
By default, no QoS policy is applied to an SRv6 TE policy.

Command reference

qos apply policy srv6-policy

Use **qos apply policy srv6-policy** to apply a QoS policy to an SRv6 TE policy.

Use **undo qos apply policy srv6-policy** to restore the default.

Syntax

```
qos apply policy policy-name srv6-policy end-point ipv6 ipv6-address color color-value  
undo qos apply policy policy-name srv6-policy end-point ipv6 ipv6-address color color-value
```

Default

No QoS policy is applied to an SRv6 TE policy.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

end-point ipv6 *ipv6-address*: Specifies an SRv6 TE policy by its end-point IPv6 address.

color *color-value*: Specifies an SRv6 TE policy by its color attribute value in the range of 0 to 4294967295.

Usage guidelines

In an L3VPN over SRv6 TE policy, you need to classify packets by VPN on the ingress of an SRv6 TE policy and then take QoS actions on matching packets, for example, traffic shaping. You can also perform QoS scheduling based on the 5-tuple of original packets of the same VPN. Applying a QoS policy to the output interface on the ingress of an SRv6 TE policy can only match the outer header information of SRv6-encapsulated packets instead of the original packet header information. This command can solve the problem.

After you execute this command, the device applies the specified QoS policy to all original packets steered to an SRv6 TE policy and perform SRv6 encapsulation and forwarding on the original packets according to the SRv6 TE policy. For more information SRv6 TE policy, see *Segment Routing Configuration Guide*.

This command takes effect only on the ingress of an SRv6 TE policy.

Only one QoS policy can be applied to an SRv6 TE policy. To apply a new QoS policy to an SRv6 TE policy that has one QoS policy applied, first execute the **undo qos apply policy srv6-policy** command.

Examples

Bind SRv6 TE policy with end-point IPv6 address 1000:1 and color attribute 10 to QoS policy **aaa**.

```
<Sysname> system-view
```

```
[Sysname] qos apply policy aaa srv6-policy end-point ipv6 1000:1 color 10
```

reset qos policy srv6-policy

Use **reset qos policy srv6-policy** to clear the statistics information about the traffic matching the QoS policy bound to an SRv6 TE policy.

Syntax

reset qos policy srv6-policy end-point ipv6 *ipv6-address* **color** *color-value*

Views

User view

Predefined user roles

network-admin

Parameters

end-point ipv6 *ipv6-address*: Specifies an SRv6 TE policy by its end-point IPv6 address.

color *color-value*: Specifies an SRv6 TE policy by its color attribute value in the range of 0 to 4294967295.

Usage guidelines

After you bind an SRv6 TE policy to a QoS policy, the device will automatically collect statistics on the traffic that matches the rules in the QoS policy. To clear the statistics information, execute this command.

Examples

Clear the statistics information about the traffic matching the QoS policy bound to an SRv6 TE policy.

```
<Sysname> reset qos policy srv6-policy end-point ipv6 1000::1 color 10
```

display qos policy srv6-policy

Use **display qos policy srv6-policy** to display QoS policies bound to SRv6 TE policies.

Syntax

In standalone mode:

display qos policy srv6-policy [**end-point ipv6** *ipv6-address* **color** *color-value*] **outbound**

In IRF mode:

display qos policy srv6-policy [**end-point ipv6** *ipv6-address* **color** *color-value*] [**slot** *slot-number*] **outbound**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

end-point ipv6 *ipv6-address*: Specifies an SRv6 TE policy by its endpoint IPv6 address.

color *color-value*: Specifies an SRv6 TE policy by its color attribute value in the range of 0 to 4294967295.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies bound to SRv6 TE policies for all member device. (In IRF mode.)

Usage guidelines

If you do not specify the **end-point ipv6** or **color** keyword when executing this command, the command displays QoS policies bound to all SRv6 TE policies.

Examples

Displays QoS policies bound to all SRv6 TE policies.

```
<Sysname> display qos policy srv6-policy outbound
  Direction: Outbound
  Policy: 1
  Classifier: 1
    Operator: AND
  Rule(s) :
    If-match acl 2000
  Behavior: 1
```



```

Marking:
  Remark dscp 3
Committed Access Rate:
  CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
  Green action : pass
  Yellow action : pass
  Red action   : discard
  Green packets : 0 (Packets) 0 (Bytes)
  Yellow packets: 0 (Packets) 0 (Bytes)
  Red packets   : 0 (Packets) 0 (Bytes)
Classifier: 2
  Operator: AND
  Rule(s) :
    If-match protocol ipv6
  Behavior: 2
    Filter enable: Permit
    Marking:
      Remark dscp 3
Classifier: 3
  Operator: AND
  Rule(s) :
    -none-
  Behavior: 3
    -none-

```

Table 3 Command output

Field	Description
Direction	Direction in which the QoS policy is applied. In the current software version, only the outbound direction is supported.
Type	Policy application type, Enhancement or Extension . This field is not displayed if no type is specified when the policy is applied.
Preorder	The order a QoS policy is executed.
Green packets	Green packet statistics.
Yellow packets	Yellow packet statistics.
Red packets	Red packet statistics.

New feature: SRv6 service chain

Creating an SRv6 service chain

Creating an SRv6 service chain in static proxy mode

About this task

Perform this task on an SFF to configure an End.AS SID to associate an SF with the SFF, create an SRv6 service chain in static proxy mode, and enter SRv6 service chain static proxy view.

In SRv6 service chain static proxy view, specify the protocol type of original packets supported by the SFF. If you do not specify a protocol type, the SFF cannot forward the original packets to the SF associated with the SFF.

Restrictions and guidelines

In a dualhoming protection scenario, the End.AS SID and End SID on each SFF must belong to different locators.

An SFF can forward the original packets of only the specified protocol type to its associated SF. If both IPv4 and IPv6 packets exist on the SRv6 SFC network, specify both the IPv4 and IPv6 protocol types in the **inner-type** command.

Procedure

1. Enter system view.
system-view
 2. Enable SRv6 and enter SRv6 view.
segment-routing ipv6
 3. Create an SRv6 locator and enter SRv6 locator view.
locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]
 4. Configure an End.AS opcode and enter SRv6 service chain static proxy view.
opcode { *opcode* | **hex** *hex-opcode* } **end-as**
 5. Allow the SFF to send original packets of the specified protocol type to the SF associated with it.
inner-type { **ipv4** | **ipv6** } *
- By default, the SFF cannot send original packets of any protocol type to an SF.

Creating an SRv6 service chain in masquerading mode

1. Enter system view.
system-view
2. Enable SRv6 and enter SRv6 view.
segment-routing ipv6
3. Configure an SRv6 locator and enter SRv6 locator view.
locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]
4. Configure an End.AM SID opcode and enter SRv6 service chain masquerading view.
opcode { *opcode* | **hex** *hex-opcode* } **end-am**

Configuring the encapsulation method for packets between a pair of SFF and SF

Configuring the packet encapsulation method for an SRv6 service chain in static proxy mode

About this task

An SF can access an SFF through a Layer 2 or Layer 3 interface. According to the interface type, you can configure the encapsulation method for packets between the SFF and SF to ensure correct packet forwarding.

An SF might have multiple VMs to load share traffic for the same application service. You can configure the packet encapsulation method multiple times for the same SRv6 service chain in static proxy mode in order to distribute the application service traffic among the VMs.

Restrictions and guidelines

To ensure correct forwarding, do not bind other services, such as VPN instances, to the input or output interface of an SRv6 service chain in static proxy mode.

An SRv6 service chain in static proxy mode supports only one packet encapsulation method. You cannot configure both Layer 2 and Layer 3 encapsulation methods for the service chain.

The same input interface cannot be shared by an SRv6 service chain in static proxy mode and an SRv6 service chain in masquerading mode.

Layer 3 encapsulation supports only Layer 3 output interfaces and Layer 3 input interfaces. VLAN interfaces cannot be used as output interfaces or input interfaces for Layer 2 encapsulation.

When you configure Layer 2 encapsulation, follow these restrictions and guidelines:

- Each SRv6 service chain in static proxy mode must have unique input interfaces, inner inbound VLAN IDs, and outer inbound VLAN IDs.
- In an SRv6 service chain in static proxy mode, the same output interface and inner and outer outbound VLAN IDs can be associated with only one input interface. If you associate different input interfaces with the same output interface and inner and outer outbound VLAN IDs for the SRv6 service chain, the most recent configuration takes effect.

For Layer 3 encapsulation, each SRv6 service chain in static proxy mode must have unique input interfaces. In the same SRv6 service chain in static proxy mode, one output interface can be associated with only one input interface.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 locator view.
locator locator-name [ipv6-prefix ipv6-address prefix-length [args args-length | static static-length] *]
4. Enter SRv6 service chain static proxy view.
opcode { opcode | hex hex-opcode } end-as
5. Configure the encapsulation method for packets forwarded between the SFF and SF. Choose one of the following tasks:

- Configure Layer 2 encapsulation for packets forwarded between the SFF and SF.
encapsulation eth out-interface *out-interface-type out-interface-number*
[**out-s-vlan** *out-svid* [**out-c-vlan** *out-cvid*]] **in-interface** *in-interface-type*
in-interface-number [**in-s-vlan** *in-svid* [**in-c-vlan** *in-cvid*]] [**dest-mac** *dest-mac*]
By default, Layer 2 encapsulation is not configured for packets forwarded between the SFF and SF.
To load share traffic, execute this command multiple times to specify multiple interfaces or VLANs.
- Configure Layer 3 encapsulation for inner IPv4 packets forwarded between the SFF and SF.
encapsulation ipv4 nexthop *nexthop-addr out-interface out-interface-type*
out-interface-number in-interface in-interface-type in-interface-number
[**symmetric-index** *index-value*]
By default, Layer 3 encapsulation is not configured for inner IPv4 packets forwarded between the SFF and SF.
To load share traffic, execute this command multiple times to specify multiple next hops.

Configuring the packet encapsulation method for an SRv6 service chain in masquerading mode

About this task

An SF can access an SFF through a Layer 2 or Layer 3 interface. According to the interface type, you can configure the encapsulation method for packets between the SFF and SF to ensure correct packet forwarding.

Restrictions and guidelines

To ensure correct forwarding, do not bind other services such as VPN instances to an interface if that interface is specified as the input or output interface of an SRv6 service chain.

An SRv6 service chain in masquerading mode supports only one packet encapsulation method. You cannot configure both the Layer 2 and Layer 3 encapsulation methods for the same SRv6 service chain in masquerading mode.

When you configure input interfaces, follow these restrictions and guidelines:

- The same input interface cannot be shared by an SRv6 service chain in static proxy mode and an SRv6 service chain in masquerading mode.
- Multiple SRv6 service chains in masquerading mode can share the same input interface.
- Layer 3 encapsulation supports only Layer 3 input interfaces. VLAN interfaces cannot be used as input interfaces for Layer 2 encapsulation.

When you configure output interfaces and outer outbound VLAN IDs, follow these restrictions and guidelines:

- Layer 3 encapsulation supports only Layer 3 output interfaces. VLAN interfaces cannot be used as output interfaces for Layer 2 encapsulation.
- For Layer 2 encapsulation, the same output interface and inner and outer outbound VLAN IDs can be associated with only one input interface in an SRv6 service chain in masquerading mode. If you associate different input interfaces with the same output interface and inner and outer outbound VLAN IDs for the SRv6 service chain, the most recent configuration takes effect.
- For Layer 3 encapsulation, one output interface can be associated with only one input interface in an SRv6 service chain in masquerading mode.

Procedure

1. Enter system view.

- system-view**
2. Enter SRv6 view.
segment-routing ipv6
 3. Enter SRv6 locator view.
locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]
 4. Enter SRv6 service chain masquerading view.
opcode { *opcode* | **hex** *hex-opcode* } **end-am**
 5. Configure the encapsulation method for packets forwarded between the SFF and SF. Choose one of the following tasks:
 - Configure Layer 2 encapsulation for packets forwarded between the SFF and SF.
encapsulation eth out-interface *out-interface-type out-interface-number*
[**out-s-vlan** *out-svid* [**out-c-vlan** *out-cvid*]] **in-interface** *in-interface-type*
in-interface-number [**in-s-vlan** *in-svid* [**in-c-vlan** *in-cvid*]]

By default, Layer 2 encapsulation is not configured for packets forwarded between an SFF and SF.
To load share traffic, execute this command multiple times to specify multiple interfaces or VLANs.
 - Configure Layer 3 encapsulation for IPv6 packets forwarded between the SFF and SF.
encapsulation ipv6 nexthop *nexthop-addr out-interface out-interface-type*
out-interface-number in-interface in-interface-type in-interface-number

By default, Layer 3 encapsulation is not configured for IPv6 packets forwarded between an SFF and SF.
To load share traffic, execute this command multiple times to specify multiple next hops.
 - Configure Layer 3 encapsulation for inner IPv6 packets forwarded between the SFF and SF.
encapsulation ipv6 nexthop *nexthop-ipv6-addr out-interface out-interface-type*
out-interface-number in-interface in-interface-type in-interface-number
[**symmetric-index** *index-value*]

By default, Layer 3 encapsulation is not configured for inner IPv6 packets forwarded between the SFF and SF.
To load share traffic, execute this command multiple times to specify multiple next hops.

Configuring packet reencapsulation parameters for an SRv6 service chain in static proxy mode

About this task

In static proxy mode, when packets return back to an SFF after they are processed by the SF associated with the SFF, they do not have an outer IPv6 header or SRH. To continue forwarding the packets in the SRv6 service chain network, the SFF must reencapsulate an SRH and outer IPv6 header to the packets. Perform this task to configure packet reencapsulation parameters on the SFF.

When the SFF receives packets forwarded from its associated SF, it searches for a matching service chain in static proxy mode based on the input interface of the packets. Then, the SFF adds an SRH and outer IPv6 header to the packets. The SRH contains the SID list configured for the service chain by using the **cache list** command. The destination address in the outer IPv6 header is the SID next to the local End.AS SID in the SID list. The source address in the outer IPv6 header is the source IPv6 address manually specified by using the **cache source-address** command.

Restrictions and guidelines

Specify the SID value of each node in the forwarding path according to the number of hops to the source node. The fewer the hops to the source node, the closer the SID position to the front of the SID list.

To avoid loops, each SID in the specified SID list must be unique.

The SID list must contain a minimum of two SIDs and must contain End.AS SIDs. The last SID in the SID list must be an End.DT4 SID or End.DT6 SID.

The explicit path of the specified SID list must be consistent with the end-to-end path in the SRv6 TE policy on the SC.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 locator view.
locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]
4. Enter SRv6 service chain static proxy view.
opcode { *opcode* | **hex** *hex-opcode* } **end-as**
5. Specify the source IPv6 address that will be reencapsulated to the packets received from the SF associated with the SFF.
cache source-address *ipv6-address*
By default, no source IPv6 address is specified for the SFF to reencapsulate the packets received from its associated SF. The SFF discards the packets.
6. Specify the SID list that will be reencapsulated to the packets received from the SF associated with the SFF.
cache list *sid-list*
By default, no SID list is specified for the SFF to reencapsulate the packets received from its associated SF.

Configuring the DiffServ mode for an SRv6 service chain in static proxy mode

About this task

In static proxy mode, perform this task on an SFF to configure the DiffServ mode for packets forwarded between the SFF and its associated SF. By default, the DiffServ mode for an SRv6 service chain in static proxy mode is uniform. If you set the mode to pipe, you must also specify the service class and color.

- **Pipe mode**—In this mode, packets are processed as follows:
 - In the inbound direction (from SF to SFF), the SFF ignores the IP precedence or DSCP value in the incoming packets. Instead, the SFF uses the specified service class as the priority and uses the specified color as the color flag when it reencapsulates the packets as SRv6 packets. In the SRv6 network, devices perform QoS scheduling for the packets based on the specified service class and color.
 - In the outbound direction (from SFF to SF), the SFF removes the outer IPv6 header and SRH without modifying the IP precedence, DSCP, or color in the original packets.

- **Uniform mode**—In this mode, packets are processed as follows:
 - In the inbound direction (from SF to SFF), the SFF maps the IP precedence or DSCP value in the original packets to the outer IPv6 header when it reencapsulates the packets. The color of the original packets is not mapped to the outer IPv6 header.
 - In the outbound direction (from SFF to SF), the SFF removes the outer IPv6 header and SRH from outgoing packets. Then, the SFF maps the priority value in the outer IPv6 header to the IP precedence or DSCP of the original packets. The color of the outer IPv6 header is not mapped to the original packets.

Restrictions and guidelines

For more information about IP precedence, DSCP, and color, see QoS configuration in *ACL and QoS Configuration Guide*.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 locator view.
locator locator-name [ipv6-prefix ipv6-address prefix-length [args args-length | static static-length] *]
4. Enter SRv6 service chain static proxy view.
opcode { opcode | hex hex-opcode } end-as
5. Configure the DiffServ mode for the SRv6 service chain in static proxy mode.
sfc diffserv-mode pipe service-class color
By default, the DiffServ mode is uniform for an SRv6 service chain in static proxy mode.

Configuring the TTL mode for an SRv6 service chain in static proxy mode

About this task

In static proxy mode, perform this task on an SFF to configure the TTL mode for packets forwarded back to the SFF from its associated SF.

- **Uniform mode**—When packets are forwarded back to the SFF, the SFF decreases the TTL value in the original packets by 1 and encapsulates the TTL to the reencapsulated outer IPv6 header.
- **Pipe mode**—When packets are forwarded back to the SFF, the SFF decreases the specified TTL value by 1 and encapsulates the TTL to the reencapsulated outer IPv6 header.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 locator view.
locator locator-name [ipv6-prefix ipv6-address prefix-length [args args-length | static static-length] *]
4. Enter SRv6 service chain static proxy view.

opcode { *opcode* | **hex** *hex-opcode* } **end-as**

5. Configure the TTL mode for the SRv6 service chain in static proxy mode.

sfc ttl-mode pipe *ttl-value*

By default, the TTL mode is uniform for an SRv6 service chain in static proxy mode.

Configuring dualhoming protection for an SRv6 service chain in static proxy mode

Restrictions and guidelines

The End.AS SID and End SID on an SFF must belong to different locators.

Make sure the SFFs in a dualhoming protection scenario are configured with the same primary and backup End.AS opcodes.

Make sure the static SIDs on the SFFs do not conflict with each other.

Procedure

1. Enter system view.

system-view

2. Enter SRv6 view.

segment-routing ipv6

3. Specify the End SID of the peer SFF as the backup peer SID.

proxy peer-sid *peer-sid*

By default, no backup peer SID is specified for dualhoming protection.

In a dualhoming protection scenario, specify the End SID of the peer SFF as the backup peer SID on each SFF.

4. Enter SRv6 locator view.

locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]

5. Enter SRv6 service chain static proxy view.

opcode { *opcode* | **hex** *hex-opcode* } **end-as**

6. Specify a backup End.AS SID opcode for SRv6 service chain dualhoming protection in static proxy mode.

backup-opcode { *func-opcode* | **hex** *hex-func-opcode* }

By default, no backup End.AS SID opcode is specified for SRv6 service chain dualhoming protection in static proxy mode.

The primary and backup End.AS SIDs on both SFFs must belong to the same locator. Use different opcodes to distinguish the primary and backup End.AS SIDs on the SFFs.

Configuring bypass protection for an SRv6 service chain in static proxy mode

Restrictions and guidelines

Dualhoming protection takes precedence over bypass protection. If dualhoming protection is not available or fails, bypass protection applies.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 locator view.
locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]
4. Enter SRv6 service chain static proxy view.
opcode { *opcode* | **hex** *hex-opcode* } **end-as**
5. Enable bypass and specify a bypass End.AS SID.
bypass [**sid** *ipv6-address*]

By default, bypass is disabled.

To ensure correct packet forwarding when the SF associated with the SFF is unreachable and the network does not have a bypass SF, enable bypass without specifying a bypass End.AS SID. In this case, the SFF skips the End.AS SID of the current SF and uses the next SID in the SRH as the next hop destination address. The data traffic is forwarded to the tail node according to the SRH.

Using static BFD in echo packet mode to detect SF reachability

About this task

Perform this task on an SFF to use a static BFD session in echo packet mode to detect the reachability of the SF associated with that SFF. When the SF is unreachable, the system can quickly trigger dualhoming protection or bypass protection for the SRv6 service chain in static proxy mode.

Restrictions and guidelines

Layer 2 encapsulation does not support this feature in the current software version.

You only need to create a static BFD session on the local SFF.

When creating a static BFD session on an SFF, you must specify the IPv4 address of the SF associated with that SFF as the peer address of the session. The system only checks the IPv4 address format and does not validate it. To ensure successful static BFD session establishment, make sure the peer IP address and source IP address are correct for the session.

The local discriminator of each static BFD session must be unique.

A static BFD session uses the following rules to select the source address for echo packets:

1. Uses the source address specified when the static BFD session was created (by using **source-ip** or **source-ipv6** keyword in the **bfd static** command).
2. Uses the source address specified by using the **bfd echo-source-ip** or **bfd echo-source-ipv6** command if no source address specified when the static BFD session was created.
3. Uses the IPv4 or IPv6 address of the packet output interface if no source address is selected after the previous steps.

As a best practice, specify a source IP address when creating a static BFD session in echo packet mode.

For more information about the commands in this section, see BFD commands in *High Availability Command Reference*.

Procedure

1. Enter system view.

system-view

2. (Optional.) Configure the source IP address of echo packets.

- o Configure the source IPv4 address of echo packets.

bfd echo-source-ip *ip-address*

By default, no source IPv4 address is configured for echo packets.

- o Configure the source IPv6 address of echo packets.

bfd echo-source-ipv6 *ipv6-address*

By default, no source IPv6 address is configured for echo packets.

3. Create a static BFD session and enter static BFD session view.

- o IPv4:

bfd static *session-name* [**peer-ip** *ipv4-address* **interface** *interface-type* *interface-number* **destination-ip** *ipv4-address* [**source-ip** *ipv4-address*] **one-arm-echo** [**discriminator** **auto**]]

- o IPv6:

bfd static *session-name* [**peer-ipv6** *ipv6-address* **interface** *interface-type* *interface-number* **destination-ipv6** *ipv6-address* [**source-ipv6** *ipv6-address*] **one-arm-echo** [**discriminator** **auto**]]

4. (Optional.) Specify the local discriminator for the static BFD session.

discriminator local *local-value*

By default, no local discriminator is specified for a static BFD session.

Use this command only if no local discriminator is specified for a static BFD session when the session is created.

Command reference

New command: backup-opcode

Use **backup-opcode** to specify a backup End.AS SID opcode for SRv6 service chain dualhoming protection in static proxy mode.

Use **undo backup-opcode** to restore the default.

Syntax

backup-opcode { *func-opcode* | **hex** *hex-func-opcode* }

undo backup-opcode

Default

No backup End.AS SID opcode is configured for SRv6 service chain dualhoming protection in static proxy mode.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

func-opcode: Specifies a backup End.AS SID opcode for SRv6 service chain dualhoming protection in static proxy mode. The value range for the opcode is 1 to $2^{\text{static-length}} - 1$. The *static-length* argument is configured by using the **locator** command.

hex hex-func-opcode: Specifies a backup End.AS SID opcode in hexadecimal notation for SRv6 service chain dualhoming protection in static proxy mode. The *hex-func-opcode* argument represents the backup End.AS SID opcode in hexadecimal notation.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

Use this command on an SFF to specify a backup End.AS SID in a dualhoming protection scenario. The primary and backup End.AS SIDs must belong to the same locator. To distinguish the primary and backup End.AS SIDs, specify different opcodes in the locator on the SFFs. When the primary SFF cannot reach the SF, it removes the outer IPv6 header and SRH to decapsulate packets. Then, the primary SFF reencapsulates a new outer IPv6 header and SRH to the packets. The SRH contains the backup End.AS SID configured by using this command and the End SID of the backup SFF specified by using the **proxy peer-sid** command. In the outer IPv6 header, the destination address is the End SID of the backup SFF.

Before using the **backup-opcode** command, use the **proxy peer-sid** command to specify the End SID of the backup SFF.

Static SIDs on the redundant SFFs cannot conflict with each other. The SFFs must be configured with the same locator and the same backup SID opcode.

Examples

Set the backup End.AS SID opcode to 12 for SRv6 service chain dualhoming protection in static proxy mode.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] proxy peer-sid 1:2:3::3:4
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] backup-opcode 12
```

Related commands

proxy peer-sid

New command: bypass

Use **bypass** to enable bypass and specify a bypass End.AS SID for an SRv6 service chain in static proxy mode.

Use **undo bypass** to disable bypass and cancel the bypass End.AS SID configuration for an SRv6 service chain in static proxy mode.

Syntax

bypass [**sid** *ipv6-address*]

undo bypass [**sid** *ipv6-address*]

Default

Bypass is disabled.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

sid *ipv6-address*: Specifies a bypass End.AS SID. The *ipv6-address* argument represents the End.AS SID. If you do not specify a bypass End.AS SID, this command only enables bypass and the system does not forward packets to a bypass SF.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

If you do not use this command on an SFF, the SFF discards packets destined for its associated SF when the SF fails or the SFF cannot reach the SF.

If you use this command on an SFF, the SFF forwards packets as follows when the SF fails or the SFF cannot reach its associated SF:

- If you do not specify the **sid** *ipv6-address* option, the SFF decapsulates the packets and reencapsulates a new SRH and outer IPv6 header to the packets. The SRH contains the SID list specified by using the **cache list** command. The reencapsulated packets will skip the SF and be forwarded as in a standard SRv6 packet forwarding process.
- If you specify the **sid** *ipv6-address* option, the SFF decapsulates the packets and reencapsulates a new SRH and outer IPv6 header to the packets. The SID list in the SRH contains only the bypass End.AS SID specified by using the **bypass** command. The destination address of the reencapsulated packets is the bypass End.AS SID. The packets are forwarded to the backup SFF from the local SFF.

Dualhoming protection takes precedence over bypass protection. If dualhoming protection is not available or fails, bypass protection applies.

Examples

Enable bypass and specify bypass End.AS SID **7::8** for an SRv6 service chain in static proxy mode.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] bypass sid 7::8
```

New command: cache list

Use **cache list** to specify the SID list that will be added to the packets forwarded back to an SFF from the SF associated with that SFF.

Use **undo cache list** to delete the SID list or specific SIDs that will be added to the packets forwarded back to an SFF from the SF associated with that SFF.

Syntax

cache list *sid-list*

undo cache list [*sid-list*]

Default

No SID list is specified for an SFF to encapsulate the packets forwarded back from its associated SF.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

sid-list: Specifies a list of space-separated SIDs. The SID list can contain up to n SIDs.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

The packets forwarded back to an SFF from its associated SF do not have an outer IPv6 header or SRH. The SFF searches for a matching service chain for the packets according to the packet input interface or the packet input interface and inbound VLANs. Then, the SFF adds an SRH and outer IPv6 header to the packets. The SRH contains the SID list configured by using this command for the matching service chain. In the outer IPv6 header, the destination IPv6 address is the SID next to the local End.AS SID in the SID list.

When you configure the SID list, follow these restrictions and guidelines:

- Specify the SID value of each node in the forwarding path according to the number of hops to the source node. The fewer the hops to the source node, the more front the SID position in the SID list.
- To avoid loops, each SID in the SID list must be unique.
- The SID list must have a minimum of two SIDs and the last SID must be an End.DT4 SID or End.DT6 SID. In addition, the SID list must include the local End.AS SID.
- The explicit path of the SID list must be consistent with the end-to-end path in the SRv6 TE policy on the SC.

If you do not specify an SID for the **undo cache list** command, the command deletes all SIDs from the SID list.

Examples

Configure the SFF to encapsulate SID list 1::1, 2::2, 3::3, 4::4, 100::12, 6::6, 7::7, 8::8, and 9::9 to the packets forwarded back to the SFF from its associated SF.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] cache list 1::1 2::2 3::3 4::4
100::12 6::6 7::7 8::8 9::9
```

New command: cache source-address

Use **cache source-address** to specify the source IPv6 address that will be added to the packets forwarded back to an SFF from the SF associated with that SFF.

Use **undo cache source-address** to restore the default.

Syntax

cache source-address *ipv6-address*

undo cache source-address

Default

No source IPv6 address is specified for an SFF to encapsulate the packets forwarded back from its associated SF.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies an IPv6 address.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

To ensure correct packet encapsulation and forwarding, execute this command to specify a source IPv6 address for an SFF to encapsulate the packets forwarded back from its associated SF. If you do not execute this command, the SFF will discard the packets forwarded back from its associated SF.

One SFF can associate only with one SF. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify IPv6 address 1:2::3:4 as the source IPv6 address that will be added to the packets forwarded back to the SFF from its associated SF.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] cache source-address 1:2::3:4
```

New command: display segment-routing ipv6 sfc forwarding

Use **display segment-routing ipv6 sfc forwarding** to display forwarding entry information about SRv6 service chains in static proxy mode.

Syntax

```
display segment-routing ipv6 sfc forwarding [ locator locator-name ] [ opcode operation-code ] [ nid-value ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

locator *locator-name*: Specifies an SRv6 locator by its name, a case-sensitive string of 1 to 31 characters. If you do not specify an SRv6 locator, this command displays SRv6 service chain forwarding entry information for all SRv6 locators.

opcode *operation-code*: Specifies an opcode. The *operation-code* argument represents the opcode of an SRv6 End.AS SID in the specified SRv6 locator. If you do not specify an opcode, this command displays SRv6 service chain forwarding entry information for all opcodes in the specified SRv6 locator.

nid-value: Specifies a forwarding entry by its ID. If you do not specify a forwarding entry, this command displays information for all SRv6 service chain forwarding entries.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

Examples

Display forwarding entry information about SRv6 service chains in static proxy mode.

```
<Sysname> display segment-routing ipv6 sfc forwarding
Total forwarding entries: 1
```

```
NID                : 2153775106
Locator name/Opcode : aaa/1
Type               : Cache list
Path Count         : 2
Interface          : GE1/0/1
Next hop           : FE80::6CCE:CBFF:FE91:206
Interface          : GE1/0/1.1
Next hop           : FE80::6CCE:CBFF:FE91:207
```

Table 4 Command output

Field	Description
Total forwarding entries	Total number of SRv6 service chain forwarding entries.
NID	SRv6 service chain forwarding entry ID.
Locator name/Opcode	End.AS SID locator name and opcode.
Type	Forwarding entry generation method: • Cache list—Forwarding entry generated based on the cache list configuration. • Bypass—Forwarding entry generated based on the bypass protection configuration. • Backup opcode—Forwarding entry generated based on the backup End.AS SID opcode configuration for dualhoming protection.
Path Count	Number of output paths.
Interface	Output interface abbreviation.
Next hop	Next hop address.

New command: encapsulation eth out-interface

Use **encapsulation eth out-interface** to configure Layer 2 encapsulation for packets forwarded between a pair of SFF and SF.

Use **undo encapsulation eth out-interface** to remove Layer 2 encapsulation configuration for packets forwarded between a pair of SFF and SF.

Syntax

In SRv6 service chain static proxy view:

```
encapsulation eth out-interface out-interface-type out-interface-number [ out-s-vlan out-svid [ out-c-vlan out-cvid ] ] in-interface in-interface-type in-interface-number [ in-s-vlan in-svid [ in-c-vlan in-cvid ] ] [ dest-mac dest-mac ]
```

undo encapsulation eth out-interface *out-interface-type out-interface-number* [**out-s-vlan** *out-svid* [**out-c-vlan** *out-cvid*]] **in-interface** *in-interface-type in-interface-number* [**in-s-vlan** *in-svid* [**in-c-vlan** *in-cvid*]]

In SRv6 service chain masquerading view:

encapsulation eth out-interface *out-interface-type out-interface-number* [**out-s-vlan** *out-svid* [**out-c-vlan** *out-cvid*]] **in-interface** *in-interface-type in-interface-number* [**in-s-vlan** *in-svid* [**in-c-vlan** *in-cvid*]]

undo encapsulation eth out-interface *out-interface-type out-interface-number* [**out-s-vlan** *out-svid* [**out-c-vlan** *out-cvid*]] **in-interface** *in-interface-type in-interface-number* [**in-s-vlan** *in-svid* [**in-c-vlan** *in-cvid*]]

Default

Layer 2 encapsulation is not configured for an SFF to encapsulate the packets forwarded back from the SF associated with that SFF.

Views

SRv6 service chain static proxy view

SRv6 service chain masquerading view

Predefined user roles

network-admin

Parameters

out-interface-type out-interface-number: Specifies an output interface by its type and number.

out-s-vlan *out-svid*: Specifies an outer VLAN ID for outgoing packets from the SFF to the SF. The *out-svid* argument represents the outer VLAN ID, in the range of 1 to 4094. If you do not specify an outer VLAN ID, the outer VLAN ID is the PVID of the output interface.

out-c-vlan *out-cvid*: Specifies an inner VLAN ID for outgoing packets from the SFF to the SF. The *out-cvid* argument represents the inner VLAN ID, in the range of 1 to 4094. If you do not specify an inner VLAN ID, the outgoing packets do not have an inner VLAN ID. Only the outer VLAN ID is encapsulated into the outgoing packets.

in-interface *in-interface-type in-interface-number*: Specifies an input interface by its type and number.

in-s-vlan *in-svid*: Specifies an outer VLAN ID for incoming packets from the SF to the SFF. The *in-svid* argument represents the outer VLAN ID, in the range of 1 to 4094. If you do not specify an outer VLAN ID, the outer VLAN ID is the PVID of the input interface.

in-c-vlan *in-cvid*: Specifies an inner VLAN ID for incoming packets from the SF to the SFF. The *in-cvid* argument represents the inner VLAN ID, in the range of 1 to 4094. If you do not specify an inner VLAN ID, the incoming packets do not have an inner VLAN ID. Only the outer VLAN ID is encapsulated into the incoming packets.

dest-mac *dest-mac*: Specifies the destination MAC address that will be encapsulated to the packets sent from the SF to the remote redundant SFF in a dualhoming protection scenario. The *dest-mac* argument represents the destination MAC address, in the format of H-H-H. The MAC address cannot be the all-F or all-zero MAC address or a multicast MAC address. If you do not specify a destination MAC address, the destination MAC address for the packets forwarded from the SF is the MAC address of the input interface on the local SFF. This option is available only in SRv6 service chain static proxy view.

Usage guidelines



IMPORTANT:

If an interface has been specified as an input or output interface of an SRv6 service chain, do not configure other services on that interface. Any violation might cause forwarding issues.

Use this command if the SFF is connected to the SF through a Layer 2 Ethernet interface, Layer 3 Ethernet interface, or Layer 3 Ethernet subinterface. The **out-interface** *out-interface-type out-interface-number* and **in-interface** *in-interface-type in-interface-number* options specify output and input interfaces, respectively, on the SFF. The output interface is the interface through which packets are forwarded from the SFF to the SF. The input interface is the interface through which the SFF receives packets from the SF. The output and input interfaces can be the same interface or different interfaces.

When you use this command, follow these restrictions and guidelines:

- If the output and input interfaces are Layer 3 Ethernet subinterfaces, follow these restrictions and guidelines to ensure correct packet forwarding:
 - If this command only specifies the outer VLAN IDs, the inbound and outbound outer VLAN IDs must be the same as the termination VLAN IDs specified by using the **vlan-type dot1q vid** command on each Layer 3 Ethernet subinterface.
 - If this command specifies both the inner and outer VLAN IDs, the inner and outer VLAN IDs specified for each subinterface must be the same as the termination inner and outer VLAN IDs specified by using the **vlan-type dot1q vid second-dot1q** command on these subinterfaces.
- If the output and input interfaces are Layer 3 Ethernet interfaces, do not specify the **out-s-vlan** *out-svid*, **in-s-vlan** *in-svid*, **out-c-vlan** *out-cvid*, or **in-c-vlan** *in-cvid* option.

Each SRv6 service chain in static proxy mode must have unique input interfaces, inbound inner VLAN IDs, and inbound outer VLAN IDs. The same input interface cannot be shared by an SRv6 service chain in static proxy mode and an SRv6 service chain in masquerading mode.

In an SRv6 service chain, the same output interface and outbound inner and outer VLAN IDs can be associated with only one input interface. If you associate different input interfaces with the same output interface and outbound inner and outer VLAN IDs for the SRv6 service chain, the most recent configuration takes effect.

In a dualhoming protection scenario for an SRv6 service chain in static proxy mode, the local SFF and its associated SF do not know the MAC address of the remote redundant SFF. For the SF to forward traffic back to the remote redundant SFF instead of the local SFF, use the **dest-mac** *dest-mac* option on the local SFF. Make sure the destination MAC address specified by using this option is the MAC address of the input interface on the remote redundant SFF. The outgoing traffic is forwarded from the local SFF to the SF and the incoming traffic is forwarded from the SF to the remote redundant SFF. As a result, outgoing traffic and incoming traffic are distributed to different SFFs for load sharing. The **dest-mac** *dest-mac* option is not available for an SRv6 service chain in masquerading mode.

If the SF has multiple VMs to process service chain traffic, execute this command multiple times for the same SRv6 service chain to specify multiple output interfaces or outbound VLANs. This operation distributes the traffic of an application service to multiple VMs for load sharing. The maximum number of load sharing links varies by device model.

For an SRv6 service chain in static proxy mode, the **encapsulation eth out-interface** command is mutually exclusive with the **encapsulation ipv4 nexthop** and **encapsulation ipv6 nexthop** commands. An SRv6 service chain in static proxy mode supports only one packet encapsulation method.

For an SRv6 service chain in masquerading mode, the **encapsulation eth out-interface** command is mutually exclusive with the **encapsulation ipv6 nexthop** command. An SRv6 service chain in masquerading mode supports only one packet encapsulation method.

Examples

For an SRv6 service chain in static proxy mode, configure Layer 2 encapsulation for packets forwarded between the SFF and its associated SF. The output interface is GigabitEthernet 1/0/1 and the input interface is GigabitEthernet 1/0/1. The outbound outer VLAN ID is 2, the inbound outer VLAN ID is 4, the outbound inner VLAN ID is 3, and the inbound inner VLAN ID is 5.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] encapsulation eth out-interface
gigabitethernet 1/0/1 out-s-vlan 2 out-c-vlan 3 in-interface gigabitethernet 1/0/1
in-s-vlan 4 in-c-vlan 5
```

For an SRv6 service chain in static proxy mode, configure Layer 2 encapsulation for packets forwarded between the SFF and its associated SF. The output interface is GigabitEthernet 1/0/1 and the input interface is GigabitEthernet 1/0/1. The outbound outer VLAN ID is 2, the inbound outer VLAN ID is 4, the outbound inner VLAN ID is 3, and the inbound inner VLAN ID is 5. The destination MAC address is abc-de-89.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] encapsulation eth out-interface
gigabitethernet 1/0/1 in-s-vlan 2 out-c-vlan 3 in-interface gigabitethernet 1/0/1
in-s-vlan 4 in-c-vlan 5 dest-mac abc-de-89
```

For an SRv6 service chain in masquerading mode, configure Layer 2 encapsulation for packets forwarded between the SFF and its associated SF. The output interface is GigabitEthernet 1/0/1 and the input interface is GigabitEthernet 1/0/1. The outbound outer VLAN ID is 2, the inbound outer VLAN ID is 4, the outbound inner VLAN ID is 3, and the inbound inner VLAN ID is 5.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-am
[Sysname-segment-routing-ipv6-locator-test-endam-32] encapsulation eth out-interface
gigabitethernet 1/0/1 out-s-vlan 2 out-c-vlan 4 in-interface gigabitethernet 1/0/1
in-s-vlan 4 in-c-vlan 5
```

Related commands

encapsulation ipv4 nexthop

encapsulation ipv6 nexthop

New command: encapsulation ipv4 nexthop

Use **encapsulation ipv4 nexthop** to configure Layer 3 encapsulation for inner IPv4 packets forwarded between a pair of SFF and SF.

Use **undo encapsulation ipv4 nexthop** to remove Layer 3 encapsulation configuration for inner IPv4 packets forwarded between a pair of SFF and SF.

Syntax

encapsulation **ipv4** **nexthop** *nexthop-addr* **out-interface** *out-interface-type*
out-interface-number **in-interface** *in-interface-type* *in-interface-number* [**symmetric-index**
index-value]

undo encapsulation ipv4 nexthop *nexthop-addr* **out-interface** *out-interface-type out-interface-number* **in-interface** *in-interface-type in-interface-number*

Default

Layer 3 encapsulation is not configured for an SFF to encapsulate the inner IPv4 packets forwarded back from the SF associated with that SFF.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

nexthop-addr: Specifies a next hop IPv4 address in dotted decimal notation.

out-interface *out-interface-type out-interface-number*: Specifies an output interface by its type and number. You can specify a VLAN interface, Layer 3 Ethernet interface, or Layer 3 Ethernet subinterface.

in-interface *in-interface-type in-interface-number*: Specifies an input interface by its type and number.

symmetric-index *index-value*: Specifies a VM by its index. To ensure that the forward traffic and backward traffic between two nodes pass through the same path, specify the same VM for the SRv6 service chains that process the traffic. The *index-value* argument represents the VM index, in the range of 1 to 4294967295. If you do not specify a VM index, the SRv6 service chain selects a VM to process forward or backward traffic according to the VM configuration order.

Usage guidelines



IMPORTANT:

If an interface has been specified as an input or output interface of an SRv6 service chain, do not configure other services on that interface. Any violation might cause forwarding issues.

This command is applicable to an SRv6 service chain in static proxy mode.

Use this command if the SFF is connected to the SF through a Layer 3 interface. The **out-interface** *out-interface-type out-interface-number* and **in-interface** *in-interface-type in-interface-number* options specify output and input interfaces, respectively, on the SFF. The output interface is the interface through which inner IPv4 packets are forwarded from the SFF to the SF. The input interface is the interface through which the SFF receives inner IPv4 packets from the SF. The output and input interfaces can be the same interface or different interfaces. One SRv6 service chain in static proxy mode must have unique input interfaces among all SRv6 service chains. In the same SRv6 service chain in static proxy view, the same output interface and next hop address can be associated only with one input interface.

If you specify the same output interface and next hop address to associate with different input interfaces in an SRv6 service chain in static proxy mode, the most recent configuration takes effect.

If multiple VMs exist on the SF, you can specify multiple input and output interfaces to distribute the traffic of an SRv6 service chain in static proxy mode among the VMs for load sharing. The maximum number of load sharing links varies by device model.

Typically, traffic in a service chain network is bidirectional. Forward traffic is the traffic from the SC to the tail node. Backward traffic is the traffic from the tail node to the SC. An SFF has two SRv6 service chains in static proxy mode in opposite directions for traffic between the SC and tail node. To ensure that the forward traffic and backward traffic are processed by the same VM when the SF has multiple VMs, specify the same VM index for the two SRv6 service chains in static proxy mode.

To specify the VM index, use this command with the **symmetric-index** *index-value* option. If you do not specify a VM index, the system automatically assigns the index of 0. In this case, an SRv6 service chain in static proxy mode selects a VM to process forward or backward traffic according to the VM configuration order. If you execute this command multiple times to specify the same VM index for the same SRv6 service chain in static proxy mode, the most recent configuration takes effect.

The **encapsulation ipv4 nexthop** command is mutually exclusive with the **encapsulation eth out-interface** command. An SRv6 service chain in static proxy mode supports only one packet encapsulation method.

Examples

Configure Layer 3 encapsulation for inner IPv4 packets forwarded between the SFF and its associated SF. The next hop address is 10.2.3.4, the output interface is GigabitEthernet1/0/1, the input interface is GigabitEthernet1/0/1, and the VM index is 10.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] encapsulation ipv4 nexthop
10.2.3.4 out-interface gigabitethernet 1/0/1 in-interface gigabitethernet 1/0/1
symmetric-index 10
```

Configure Layer 3 encapsulation for inner IPv4 packets forwarded between the SFF and its associated SF. The next hop address is 10.2.3.4, the output interface is VLAN-interface 10, the input interface is VLAN-interface 10, and the VM index is 10.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] encapsulation ipv4 nexthop
10.2.3.4 out-interface vlan-interface 10 in-interface vlan-interface 10 symmetric-index
10
```

Related commands

encapsulation eth out-interface

New command: encapsulation ipv6 nexthop

Use **encapsulation ipv6 nexthop** to configure Layer 3 encapsulation for IPv6 packets forwarded between a pair of SFF and SF.

Use **undo encapsulation ipv6 nexthop** to remove Layer 3 encapsulation configuration for IPv6 packets forwarded between a pair of SFF and SF.

Syntax

encapsulation ipv6 nexthop *nexthop-ipv6-addr* **out-interface** *out-interface-type out-interface-number* **in-interface** *in-interface-type in-interface-number* [**symmetric-index** *index-value*]

undo encapsulation ipv6 nexthop *nexthop-ipv6-addr* **out-interface** *out-interface-type out-interface-number* **in-interface** *in-interface-type in-interface-number*

Default

Layer 3 encapsulation is not configured for an SFF to encapsulate the IPv6 packets forwarded back from the SF associated with that SFF.

Views

SRv6 service chain proxy view

SRv6 service chain masquerading view

Predefined user roles

network-admin

Parameters

nexthop-ipv6-addr: Specifies a next hop IPv6 address.

out-interface *out-interface-type out-interface-number*: Specifies an output interface by its type and number. You can specify a VLAN interface, Layer 3 Ethernet interface, or Layer 3 Ethernet subinterface.

in-interface *in-interface-type in-interface-number*: Specifies an input interface by its type and number.

symmetric-index *index-value*: Specifies a VM by its index. To ensure that the forward traffic and backward traffic between two nodes pass through the same path, specify the same VM for the SRv6 service chains that process the traffic. The *index-value* argument represents the VM index, in the range of 1 to 4294967295. If you do not specify a VM index, the SRv6 service chain selects a VM to process forward or backward traffic according to the VM configuration order.

Usage guidelines



IMPORTANT:

If an interface has been specified as an input or output interface of an SRv6 service chain, do not configure other services on that interface. Any violation might cause forwarding issues.

Use this command if the SFF is connected to the SF through a Layer 3 interface. The **out-interface** *out-interface-type out-interface-number* and **in-interface** *in-interface-type in-interface-number* options specify output and input interfaces, respectively, on the SFF. The output interface is the interface through which IPv6 packets are forwarded from the SFF to the SF. The input interface is the interface through which the SFF receives IPv6 packets from the SF. The output and input interfaces can be the same interface or different interfaces. One SRv6 service chain in masquerading view or static proxy view must have unique input interfaces among all SRv6 service chains. In the same SRv6 service chain in masquerading view or in static proxy view, the same output interface and next hop address can be associated with only one input interface. The input interfaces for different SRv6 service chains in static proxy view must be different.

If you specify the same output interface and next hop address to associate with different input interfaces for an SRv6 service chain in masquerading view or static proxy view, the most recent configuration takes effect.

If multiple VMs exist on the SF, you can specify multiple input and output interfaces to distribute the traffic of an SRv6 service chain in masquerading view or static proxy view among the VMs for load sharing. The maximum number of load sharing links varies by device model.

Typically, traffic in a service chain network is bidirectional. Forward traffic is the traffic from the SC to the tail node. Backward traffic is the traffic from the tail node to the SC. An SFF has two End.AS SIDs or two End.AM SIDs in opposite directions for traffic between the SC and tail node. To ensure that the forward traffic and backward traffic are processed by the same VM when the SF has multiple VMs, specify the same VM index for the two SRv6 service chains in static proxy mode.

To specify the VM index, use this command with the **symmetric-index** *index-value* option. If you do not specify a VM index, the system automatically assigns the index of 0. In this case, an SRv6 service chain in static proxy mode selects a VM to process forward or backward traffic according to the VM configuration order. If you execute this command multiple times to specify the same VM index for the same SRv6 service chain in masquerading view or static proxy view, the most recent configuration takes effect.

The **encapsulation ipv6 nexthop** command is mutually exclusive with the **encapsulation eth out-interface** command. An SRv6 service chain in masquerading view or static proxy view supports only one packet encapsulation method.

Examples

Configure Layer 3 encapsulation for IPv6 packets forwarded between the SFF and its associated SF. The next hop address is 1::1, the output interface is GigabitEthernet 1/0/1, and the input interface is GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-am
[Sysname-segment-routing-ipv6-locator-test-endam-32] encapsulation ipv6 nexthop 1::1
out-interface gigabitethernet 1/0/1 in-interface gigabitethernet 1/0/1
```

Related commands

encapsulation eth out-interface

New command: inner-type

Use **inner-type** to specify the protocol type of original packets that can be sent by an SFF to the SF associated with that SFF.

Use **undo inner-type** to remove the specified protocol type configuration of original packets that can be sent by an SFF to the SF associated with that SFF.

Syntax

```
inner-type { ipv4 | ipv6 } *
undo inner-type [ ipv4 | ipv6 ]
```

Default

An SFF cannot send original packets of any protocol type to an SF.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

ipv4: Specifies the IPv4 protocol type.

ipv6: Specifies the IPv6 protocol type.

Usage guidelines

Use this command on an SFF to ensure that the SFF can forward traffic to its associated SF. This command is required for an SRv6 service chain in static proxy mode.

When both IPv4 and IPv6 original packets exist in the SRv6 SFC network, configure this feature and specify both the **ipv4** and **ipv6** keywords. If you do not do so, an SFF cannot forward original packets of the non-specified protocol type (IPv4 or IPv6) to its associated SF.

If you execute the **undo inner-type** command without specifying any keyword, the command removes all the specified protocol type configuration.

Examples

Configure an SFF to send original packets of the IPv4 protocol type to the SF associated with that SFF.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] inner-type ipv4
```

New command: opcode end-am

NOTE:

Support for this command depends on the device model.

Use **opcode end-am** to configure an End.AM SID opcode in an SRv6 locator and enter SRv6 service chain masquerading view, or directly enter SRv6 service chain masquerading view if the view already exists.

Use **undo opcode** to delete an End.AM SID opcode from an SRv6 locator and delete all settings in SRv6 service chain masquerading view.

Syntax

opcode { *opcode* | **hex** *hex-opcode* } **end-am**

undo opcode { *opcode* | **hex** *hex-opcode* }

Default

No End.AM SID opcode exists in an SRv6 locator.

Views

SRv6 locator view

Predefined user roles

network-admin

Parameters

opcode: Specifies an End.AM SID opcode in the range of 1 to $2^{\text{static-length}}-1$. The *static-length* argument is specified by using the **locator** command.

hex *hex-opcode*: Specifies an SRv6 End.AM SID opcode in hexadecimal notation. The *hex-opcode* argument represents the SRv6 End.AM SID opcode in hexadecimal notation.

Usage guidelines

This command is applicable to an SRv6 service chain in masquerading mode.

To modify the End.AM SID opcode in an SRv6 locator, you must first use the **undo opcode** command to delete the original opcode.

Examples

Set the End.AM SID opcode to 32 for locator **test** and enter SRv6 service chain masquerading view.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-am
```

[Sysname-segment-routing-ipv6-locator-test-endam-32]

Related commands

locator

segment-routing ipv6

New command: opcode end-as

Use **opcode end-as** to configure an End.AS SID opcode in an SRv6 locator and enter SRv6 service chain static proxy view or enter SRv6 service chain static proxy view if the view already exists.

Use **undo opcode** to delete an End.AS SID opcode from an SRv6 locator and delete all settings in SRv6 service chain static proxy view.

Syntax

opcode { *opcode* | **hex** *hex-opcode* } **end-as**

undo opcode { *opcode* | **hex** *hex-opcode* }

Default

No End.AS SID opcode exists in an SRv6 locator.

Views

SRv6 locator view

Predefined user roles

network-admin

Parameters

opcode: Specifies an End.AS SID opcode in the range of 1 to $2^{\text{static-length}-1}$. The *static-length* argument is specified by using the **locator** command.

hex *hex-opcode*: Specifies an SRv6 End.AS SID opcode in hexadecimal notation. The *hex-opcode* argument represents the SRv6 End.AS SID opcode in hexadecimal notation.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

To modify the static End.AS SID opcode in an SRv6 locator, you must first use the **undo opcode end-as** command to delete the original opcode.

Examples

Set the End.AS SID opcode to 32 for locator **test** and enter SRv6 service chain static proxy view.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32]
```

Related commands

locator

segment-routing ipv6

New command: proxy peer-sid

Use **proxy peer-sid** to specify the End SID of one SFF as the backup peer SID of the other SFF in a dualhoming protection scenario for an SRv6 service chain in static proxy mode.

Use **undo proxy peer-sid** to restore the default.

Syntax

proxy peer-sid *peer-sid*

undo proxy peer-sid

Default

No backup peer SID is specified for dualhoming protection for an SRv6 service chain in static proxy mode.

Views

SRv6 view

Predefined user roles

network-admin

Parameters

peer-sid: Specifies the End SID of the remote redundant SFF.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

In a dualhoming protection scenario, use this command on the redundant SFFs to specify the End SID of one SFF as the backup peer SID of the other SFF. If you execute this command multiple times for an SFF, the most recent configuration takes effect.

In a dualhoming protection scenario, the End SID cannot belong to the same locator as the End.AS SID on each SFF.

Examples

In a dualhoming protection scenario for an SRv6 service chain in static proxy mode, specify the End SID (1:2:3::3:4) of the other SFF as the backup peer SID of the local SFF.

```
<Sysname> system-view
```

```
[Sysname] segment-routing ipv6
```

```
[Sysname-segment-routing-ipv6] proxy peer-sid 1:2:3::3:4
```

New command: sfc diffserv-mode

Use **sfc diffserv-mode** to configure the DiffServ mode for an SRv6 service chain in static proxy mode.

Use **undo sfc diffserv-mode** to restore the default.

Syntax

sfc diffserv-mode pipe *service-class color*

undo sfc diffserv-mode

Default

The DiffServ mode is uniform for an SRv6 service chain in static proxy mode.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

pipe: Specifies the pipe mode.

service-class: Specifies a service class. The following shows the supported service classes in ascending order of priority:

- be.
- af1.
- af2.
- af3.
- af4.
- ef.
- cs6.
- cs7.

color: Specifies a color for packets. The following shows the supported colors in ascending order of packet drop probability:

- green: Specifies the green color. The packet drop priority is 0.
- yellow: Specifies the yellow color. The packet drop priority is 1.
- red: Specifies the red color. The packet drop priority is 2.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

Use this command on an SFF to configure the DiffServ mode for packets forwarded between the SFF and its associated SF.

- **Pipe mode**—In this mode, packets are processed as follows:
 - In the inbound direction (from SF to SFF), the SFF ignores the IP precedence or DSCP value in the incoming packets. Instead, the SFF uses the specified service class as the priority and uses the specified color as the color flag when it reencapsulates the packets as SRv6 packets. In the SRv6 network, devices perform QoS scheduling for the packets based on the specified service class and color.
 - In the outbound direction (from SFF to SF), the SFF removes the outer IPv6 header and SRH without modifying the IP precedence, DSCP, or color in the original packets.
- **Uniform mode**—In this mode, packets are processed as follows:
 - In the inbound direction (from SF to SFF), the SFF maps the IP precedence or DSCP value in the original packets to the outer IPv6 header when it reencapsulates the packets. The color of the original packets is not mapped to the outer IPv6 header.
 - In the outbound direction (from SFF to SF), the SFF removes the outer IPv6 header and SRH from outgoing packets. Then, the SFF maps the priority value in the outer IPv6 header to the IP precedence or DSCP of the original packets. The color of the outer IPv6 header is not mapped to the original packets.

Examples

Set the DiffServ mode to **pipe** for an SRv6 service chain in static proxy mode, set the service class to **af1**, and set the color to **red**.

```
<Sysname> system-view
```

```
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] sfc diffserv-mode pipe af1 red
```

New command: sfc ttl-mode

Use **sfc ttl-mode** to configure the TTL mode for SRv6 service chain packets forwarded back to an SFF from its associated SF.

Use **undo sfc ttl-mode** to restore the default.

Syntax

```
sfc ttl-mode pipe ttl-value
undo sfc ttl-mode
```

Default

The TTL mode is uniform.

Views

SRv6 service chain static proxy view

Predefined user roles

network-admin

Parameters

pipe: Specifies the pipe mode.
ttl-value: Sets the TTL value, in the range of 1 to 255.

Usage guidelines

This command is applicable to an SRv6 service chain in static proxy mode.

Use this command on an SFF to configure the TTL mode for packets forwarded back to the SFF from its associated SF.

- **Uniform mode**—When packets are forwarded back to the SFF, the SFF decreases the TTL value in the original packets by 1 and encapsulates the TTL to the reencapsulated outer IPv6 header.
- **Pipe mode**—When packets are forwarded back to the SFF, the SFF decreases the specified TTL value by 1 and encapsulates the TTL to the reencapsulated outer IPv6 header.

Examples

```
# Set the TTL mode to pipe and set the TTL value to 255.
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] locator test ipv6-prefix 100:: 64 static 32
[Sysname-segment-routing-ipv6-locator-test] opcode 32 end-as
[Sysname-segment-routing-ipv6-locator-test-endas-32] sfc ttl-mode pipe 255
```

Modified command: display segment-routing ipv6 local-sid

Use **display segment-routing ipv6 local-sid** to display information about the SRv6 local SID forwarding table.

Old syntax

```
display segment-routing ipv6 local-sid { end | end-b6encaps | end-b6encapsred |  
end-b6insert | end-b6insertred | end-coc32 | end-dt2m | end-dt2u | end-dt2ul |  
end-dx2 | end-dx2l | end-m | end-op | end-t | end-x-coc32 } [ sid ]  
  
display segment-routing ipv6 local-sid { end-dt4 | end-dt46 | end-dt6 | end-dx4 |  
end-dx6 } [ sid | vpn-instance vpn-instance-name ]  
  
display segment-routing ipv6 local-sid end-x [ sid | interface interface-type  
interface-number [ nexthop nexthop-ipv6-address ] ]
```

New syntax

```
display segment-routing ipv6 local-sid { end | end-am | end-as | end-b6encaps |  
end-b6encapsred | end-b6insert | end-b6insertred | end-coc32 | end-dt2m | end-dt2u  
| end-dt2ul | end-dx2 | end-dx2l | end-m | end-op | end-t | end-x-coc32 } [ sid ]  
  
display segment-routing ipv6 local-sid { end-dt4 | end-dt46 | end-dt6 | end-dx4 |  
end-dx6 } [ sid | vpn-instance vpn-instance-name ]  
  
display segment-routing ipv6 local-sid end-x [ sid | interface interface-type  
interface-number [ nexthop nexthop-ipv6-address ] ]
```

Views

Any view

Change description

end-am: Display SRv6 local forwarding table information for End.AM SIDs.

end-as: Display SRv6 local forwarding table information for End.AS SIDs.

New feature: Configuring 8-queue PQ

Configuring 8-queue PQ

1. Enter system view.
system-view
2. Configure a PQ list. Choose the options to configure as needed:
 - Configure a protocol-based PQ list.
**qos pql pql-index protocol { ip | ipv6 } [queue-key key-value] queue
queue-number**
 - Configure an interface-based PQ list.
**qos pql pql-index inbound-interface interface-type interface-number queue
queue-number**
 - Configure a local-precedence-based PQ list.
qos pql pql-index local-precedence local-precedence-list queue queue-number
 - Configure an MPLS-EXP-based PQ list.
qos pql pql-index protocol mpls exp exp-list queue queue-number
3. (Optional.) Configure a queue as the default queue for the PQ list.
qos pql pql-index default-queue queue-number
By default, the normal queue is the default queue.
The default queue enqueues packets that do not match any criteria in a PQ list.

4. (Optional.) Set the maximum queue length for a queue in the PQ list.
- qos pql** *pql-index* **queue** *queue-number* **queue-length** *queue-length*
- By default:
- The maximum top queue length is 20.
 - The maximum middle queue length is 40.
 - The maximum normal queue length is 60.
 - The maximum bottom queue length is 80.
 - The maximum queue length for queue 3 is 80.
 - The maximum queue length for queue 2 is 80.
 - The maximum queue length for queue 1 is 100.
 - The maximum queue length for queue 0 is 100.

Command reference

Modified command: qos pql default-queue

Old syntax

qos pql *pql-index* **default-queue** { **bottom** | **middle** | **normal** | **top** }
undo qos pql *pql-index* **default-queue**

New syntax

4-queue:

qos pql *pql-index* **default-queue** { **bottom** | **middle** | **normal** | **top** }
undo qos pql *pql-index* **default-queue**

8-queue:

qos pql *pql-index* **default-queue** *queue-number*
undo qos pql *pql-index* **default-queue**

Views

System view

Change description

The 8-queue command is added, and the following argument is added:

queue-number: Specifies a queue by its number in the range of 0 to 7. Queue 0 through queue 7 are in ascending order of priority.

Modified command: qos pql inbound-interface

Old syntax

qos pql *pql-index* **inbound-interface** *interface-type* *interface-number* **queue** { **bottom** | **middle** | **normal** | **top** }
undo qos pql *pql-index* **inbound-interface** *interface-type* *interface-number*

New syntax

4-queue:

qos pql *pql-index* **inbound-interface** *interface-type* *interface-number* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **inbound-interface** *interface-type* *interface-number*

8-queue:

qos pql *pql-index* **inbound-interface** *interface-type* *interface-number* **queue** *queue-number*

undo qos pql *pql-index* **inbound-interface** *interface-type* *interface-number*

Views

System view

Change description

The 8-queue command is added, and the following argument is added:

queue-number: Specifies a queue by its number in the range of 0 to 7. Queue 0 through queue 7 are in ascending order of priority.

Modified command: qos pql local-precedence

Old syntax

qos pql *pql-index* **local-precedence** *local-precedence-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **local-precedence** *local-precedence-list*

Syntax

4-queue:

qos pql *pql-index* **local-precedence** *local-precedence-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **local-precedence** *local-precedence-list*

8-queue:

qos pql *pql-index* **local-precedence** *local-precedence-list* **queue** *queue-number*

undo qos pql *pql-index* **local-precedence** *local-precedence-list*

Views

System view

Change description

The 8-queue command is added, and the following argument is added:

queue-number: Specifies a queue by its number in the range of 0 to 7. Queue 0 through queue 7 are in ascending order of priority.

Modified command: qos pql protocol

Old syntax

qos pql *pql-index* **protocol** { **ip** | **ipv6** } [*queue-key* *key-value*] **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol** { **ip** | **ipv6** } [*queue-key* *key-value*]

New syntax

4-queue:

```
qos pql pql-index protocol { ip | ipv6 } [ queue-key key-value ] queue { bottom | middle | normal | top }
```

```
undo qos pql pql-index protocol { ip | ipv6 } [ queue-key key-value ]
```

8-queue:

```
qos pql pql-index protocol { ip | ipv6 } [ queue-key key-value ] queue queue-number
```

```
undo qos pql pql-index protocol { ip | ipv6 } [ queue-key key-value ]
```

Views

System view

Change description

The 8-queue command is added, and the following argument is added:

queue-number: Specifies a queue by its number in the range of 0 to 7. Queue 0 through queue 7 are in ascending order of priority.

Modified command: qos pql protocol mpls exp

Old syntax

```
qos pql pql-index protocol mpls exp exp-list queue { bottom | middle | normal | top }
```

```
undo qos pql pql-index protocol mpls exp exp-list
```

New syntax

4-queue:

```
qos pql pql-index protocol mpls exp exp-list queue { bottom | middle | normal | top }
```

```
undo qos pql pql-index protocol mpls exp exp-list
```

8-queue:

```
qos pql pql-index protocol mpls exp exp-list queue queue-number
```

```
undo qos pql pql-index protocol mpls exp exp-list
```

Views

System view

Change description

The 8-queue command is added, and the following argument is added:

queue-number: Specifies a queue by its number in the range of 0 to 7. Queue 0 through queue 7 are in ascending order of priority.

Modified command: qos pql queue

Old syntax

```
qos pql pql-index queue { bottom | middle | normal | top } queue-length queue-length
```

```
undo qos pql pql-index queue { bottom | middle | normal | top } queue-length
```

New syntax

4-queue:

```
qos pql pql-index queue { bottom | middle | normal | top } queue-length queue-length
```

```
undo qos pql pql-index queue { bottom | middle | normal | top } queue-length
```

8-queue:

```
qos pql pql-index queue queue-number queue-length queue-length
```

```
undo qos pql pql-index queue queue-number queue-length
```

Views

System view

Change description

The 8-queue command is added, and the following argument is added:

queue-number: Specifies a queue by its number in the range of 0 to 7. Queue 0 through queue 7 are in ascending order of priority.

New feature: Configuring an SDWAN TTE information match criterion and a VPN instance match criterion

Configuring an SDWAN TTE information match criterion and a VPN instance match criterion

About this task

Perform this task to configure an SDWAN TTE information match criterion and a VPN instance match criterion in a QoS traffic class.

Procedure

1. Enter system view.
system-view
2. Create a traffic class and enter traffic class view.
traffic classifier classifier-name [operator { and | or }]
3. Configure an SDWAN TTE information match criterion.
if-match sdwan-tte site-id site-id [device-id device-id [interface-id interface-id]]
4. Configure a VPN instance match criterion.
if-match vpn-instance vpn-name

Command reference

Modified command: if-match

Syntax

```
if-match [ not ] match-criteria
undo if-match [ not ] match-criteria
```

Views

Traffic class view

Change description

The following parameters are added:

sdwan-tte site-id <i>site-id</i> [device-id <i>device-id</i> [interface-id <i>interface-id</i>]]	Matches transport tunnel endpoint (TTE) information in SDWAN. • site-id <i>site-id</i>: Specifies a site ID in the range of 1 to 65535. • device-id <i>device-id</i>: Specifies a device ID in the range of 1 to 255. If you do not specify a device ID, all devices in the site can be matched. • interface-id <i>interface-id</i>: Specifies an interface ID in the range of 1 to 255. If you do not specify an interface ID, all SDWAN tunnel interface on the device can be matched. For more information about SDWAN, see <i>SDWAN Configuration Guide</i> .
vpn-instance <i>vpn-name</i>	Matches a VPN instance.

New feature: Simplifying the QoS configuration in a hub-spoke network

Simplifying the QoS configuration in a hub-spoke network

About this task

In the SDWAN scenario, a large number of spoke devices exist in a hub-spoke network. To configure a QoS policy for each hub-spoke SDWAN tunnel, you need to manually configure and apply a QoS policy on the hub device in the central site each time a spoke device is added for a branch site. If the QoS policies for the SDWAN tunnels from the central site to the branch sites are the same except for the rate limiting settings, you can simplify QoS policy configuration on the hub device by configuring this feature on the spoke devices.

After you configure this feature on a spoke device, the BGP IPv4 Tnl-encap-ext routes advertised by the spoke device to the peer hub device will carry the specified user profile name during data channel establishment. The specified user profile will be advertised by BGP to the peer hub device along with the TTE information. The peer hub device will apply the local user profile that has the same name as the advertised user profile to the outbound direction of the hub-spoke SDWAN tunnel. If the user profile is not configured on the peer hub device or the user profile does not contain any configuration, the SDWAN tunnel will not be affected.

Prerequisites

Before you perform this task, complete the following tasks on the hub device:

- Create the specified user profile.
- Configure QoS policy, traffic policing, traffic shaping, traffic rate limiting, or priority queue settings for the user profile as needed.

For more information about user profiles, see *Security Configuration Guide*.

Restrictions and guidelines

If the user profile applied to the outbound direction of the hub-spoke SDWAN tunnel contains QoS configuration and the QoS configuration is configured to take effect in the inbound direction, the QoS configuration will not take effect. For example, the **qos car inbound** command configured in user profile view does not take effect on the hub-spoke SDWAN tunnel.

On the hub device, execute the **qos lr outbound** command with the **peer-advertise-bandwidth** keyword specified in the view of the user profile applied to the SDWAN tunnel. This configuration enables the hub device to accept the rate limit settings advertised from the peer spoke device. If you do not do so, the traffic rate limit specified by the **qos bandwidth downstream** command on the spoke device does not take effect on the hub device. For more information about the **qos lr outbound** command in user profile view, see QoS commands in *ACL and QoS Command Reference*.

Do not configure rate limiting, traffic policing, GTS, or queue scheduling on both an SDWAN tunnel and a tunnel interface. If you apply a user profile to an SDWAN tunnel between the hub and a spoke for rate limiting, the rate limiting or GTS configured on the tunnel interface on the hub does not take effect.

Configuring the traffic rate limit on the spoke

1. Enter system view.

system-view

2. Create a UDP-encapsulated SDWAN tunnel and enter tunnel interface view.

interface tunnel *tunnel-number* mode sdwan udp [ipv6]

Configure the same tunnel mode at both sides of a tunnel. Otherwise, the tunnel cannot transmit packets correctly.

3. Specify the user profile to be applied to the outbound direction of the peer tunnel interface.

qos apply user-profile *profile-name* downstream

By default, the user profile to be applied to the outbound direction of the peer tunnel interface is not specified. For more information about this command, see QoS commands in *ACL and QoS Command Reference*.

4. (Optional.) Set the traffic rate limit to be applied to the outbound direction of the peer tunnel interface.

qos bandwidth downstream *bandwidth-value*

By default, the traffic rate limit to be applied to the outbound direction of the peer tunnel interface is not set. For more information about this command, see QoS commands in *ACL and QoS Command Reference*.

Configuring a user profile on the hub

1. Enter system view.

system-view

2. Create a user profile and enter user profile view.

user-profile *profile-name*

3. Configure traffic rate limiting settings.

qos lr outbound { **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] | **peer-advertise-bandwidth** }

By default, no traffic rate limiting settings are configured for a user profile

4. Apply a PQ list to a user profile

qos pq pql *pql-index*

By default, no PQ list is applied to a user profile.

Command reference

New command: display qos policy sdwan

Use **display qos policy sdwan** to display QoS policies applied to SDWAN tunnels.

Syntax

display qos policy sdwan tunnel *number* [**site-id** *site-id* **device-id** *device-id* **interface-id** *interface-id*] **outbound**

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

number: Specifies a tunnel interface by its number in the range of 0 to 10239.

site-id *site-id*: Specifies a site ID in the range of 1 to 65535. For more information about site ID, see SDWAN configuration in *SDWAN Configuration Guide*.

device-id *device-id*: Specifies a device ID in the range of 1 to 255. For more information about device ID, see SDWAN configuration in *SDWAN Configuration Guide*.

interface-id *interface-id*: Specifies an interface ID in the range of 1 to 255. For more information about interface ID, see SDWAN configuration in *SDWAN Configuration Guide*.

outbound: Displays the QoS policies applied to the outbound direction.

Usage guidelines

If you do not specify the TTE information in SDWAN, including site ID, device ID, and interface ID, this command displays QoS policies applied to all SDWAN tunnels. For more information about SDWAN tunnels, see SDWAN configuration in *SDWAN Configuration Guide*.

For more information about tunnel interface commands, see tunneling commands in *Layer 3—IP Services Command Reference*.

Examples

Display QoS policies applied to the outbound direction of SDWAN tunnel interface 1.

```
<Sysname> display qos policy sdwan tunnel 1 outbound
```

```
Session: Tunnell SiteID1/DevID1/IfID1
```

```
Direction: Outbound
```

```
Policy: finance
```

```
Classifier: default-class
```

```
Matched : 0 (Packets) 0 (Bytes)
```

```

Operator: AND
Rule(s) :
  If-match any
Behavior: be
  -none-
Classifier: finance
Matched : 123713988 (Packets) 13608538380 (Bytes)
Operator: AND
Rule(s) :
  If-match any
Behavior: finance
Committed Access Rate:
  CIR 1500 (kbps), CBS 93750 (Bytes), EBS 0 (Bytes)
  Green action : pass
  Yellow action : pass
  Red action   : discard
  Green packets : 14980239 (Packets) 1647826290 (Bytes)
  Yellow packets: 0 (Packets) 0 (Bytes)
  Red packets   : 108733781 (Packets) 11960715910 (Bytes)

```

Table 5 Command output

Field	Description
Session	SDWAN tunnel information. An SDWAN tunnel is uniquely identified by a tunnel interface and an SDWAN-TTE address. An SDWAN-TTE address includes the following parts: • SiteID—SDWAN site ID. • DevID—SDWAN device ID. • IfID—SDWAN interface ID.
Direction	The direction to which the QoS policy is applied.
Matched	Number of matching packets.

New command: qos apply user-profile downstream

Use **qos apply user-profile downstream** to configure the user profile to be applied to the outbound direction of the peer tunnel.

Use **undo qos apply user-profile downstream** to restore the default.

Syntax

qos apply user-profile *profile-name* **downstream**

undo qos apply user-profile *profile-name* **downstream**

Default

The user profile to be applied to the outbound direction of the peer tunnel is not configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a user profile by its name, a case-sensitive string of 1 to 31 characters. Valid characters include English letters, digits, hyphens (-), and underscores (_). The name must start with an English letter or digit and must be globally unique. The name cannot contain only digits.

Usage guidelines

Application scenario

This command is applicable to only SDWAN tunnels.

In the SDWAN scenario, a large number of spoke devices exist in a hub-spoke network. To configure a QoS policy for each hub-spoke SDWAN tunnel, you need to manually configure and apply a QoS policy on the hub device in the central site each time a spoke device is added for a branch site. If the QoS policies for the SDWAN tunnels from the central site to the branch sites are the same except for the rate limiting settings, you can simplify QoS policy configuration on the hub device by executing this command on the spoke devices.

For more information about this feature, see SDWAN configuration in *SDWAN Configuration Guide*.

Operating mechanism

After you execute this command on a spoke device, the BGP IPv4 Tnl-encap-ext routes advertised by the spoke device to the peer hub device will carry the specified user profile name during data channel establishment. The specified user profile will be advertised by BGP to the peer hub device along with the TTE information. The peer hub device will apply the local user profile that has the same name as the advertised user profile to the outbound direction of the hub-spoke SDWAN tunnel. If the user profile is not configured on the peer hub device or the user profile does not contain any configuration, the SDWAN tunnel will not be affected.

Restrictions and guidelines

Before executing this command, create the specified user profile on the hub device, and configure QoS policy, traffic policing, traffic shaping, traffic rate limiting, or priority queue settings for the user profile as needed.

If the user profile applied to the outbound direction of the hub-spoke SDWAN tunnel contains QoS configuration and the QoS configuration is configured to take effect in the inbound direction, the QoS configuration will not take effect. For example, the **qos car inbound** command configured in user profile view does not take effect on the hub-spoke SDWAN tunnel.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

On the spoke device, configure the name to **u1** for the user profile to be applied to the outbound direction of the peer tunnel.

```
<Sysname> system-view
[Sysname] interface Tunnel 2 mode sdwan udp
[Sysname-Tunnel2] qos apply user-profile u1 downstream
```

New command: reset qos policy sdwan

Use **reset qos policy sdwan** to clear the statistics information about the QoS policies applied to an SDWAN tunnel.

Syntax

reset qos policy sdwan tunnel *number* [*site-id site-id device-id device-id interface-id interface-id*] **outbound**

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

number: Specifies a tunnel interface by its number in the range of 0 to 10239.

site-id *site-id*: Specifies a site ID in the range of 1 to 65535. For more information about site ID, see SDWAN configuration in *SDWAN Configuration Guide*.

device-id *device-id*: Specifies a device ID in the range of 1 to 255. For more information about device ID, see SDWAN configuration in *SDWAN Configuration Guide*.

interface-id *interface-id*: Specifies an interface ID in the range of 1 to 255. For more information about interface ID, see SDWAN configuration in *SDWAN Configuration Guide*.

outbound: Clears the statistics about the QoS policies applied to the outbound direction.

Usage guidelines

If you do not specify the **site-id**, **device-id**, or **interface-id** keyword when executing this command, the command clears statistics information about the QoS policies applied to all SDWAN tunnels.

For more information about tunnel interface commands, see tunneling commands in *Layer 3—IP Services Command Reference*.

In the current software version, the command can clear statistics about only QoS policies applied to the outbound direction.

Examples

Clear the statistics about the QoS policies applied to the specified SDWAN tunnel.

```
<Sysname> reset qos policy sdwan tunnel 1 site-id 1 device-id 1 interface-id 1 outbound
```

Modified command: display qos tunnel-session

Old syntax

```
display qos tunnel-session interface tunnel number [ identity identity ] [ inbound | outbound ]
```

New syntax

```
display qos tunnel-session interface tunnel number [ identity identity ] [ inbound | outbound ]
```

```
display qos tunnel-session interface tunnel number [ sdwan-tte site-id site-id device-id device-id interface-id interface-id ] outbound
```

Views

Any view

Change description

The following parameters are added:

sdwan-tte site-id *site-id*: Specifies a site ID in the range of 1 to 65535. For more information about site ID, see SDWAN configuration in *SDWAN Configuration Guide*.

device-id *device-id*: Specifies a device ID in the range of 1 to 255. For more information about device ID, see SDWAN configuration in *SDWAN Configuration Guide*.

interface-id *interface-id*: Specifies an interface ID in the range of 1 to 255. For more information about interface ID, see SDWAN configuration in *SDWAN Configuration Guide*.

Modified command: reset qos tunnel-session

Old syntax

```
reset qos tunnel-session interface tunnel number [ identity identity ] [ inbound | outbound ]
```

```
reset qos tunnel-session interface tunnel number [ sdwan-tte site-id site-id device-id device-id interface-id interface-id ] outbound
```

New syntax

```
reset qos tunnel-session interface tunnel number [ sdwan-tte site-id site-id device-id device-id interface-id interface-id ] outbound
```

Views

User view

Parameters

The following parameters are added:

sdwan-tte site-id *site-id*: Specifies a site ID in the range of 1 to 65535. For more information about site ID, see SDWAN configuration in *SDWAN Configuration Guide*.

device-id *device-id*: Specifies a device ID in the range of 1 to 255. For more information about device ID, see SDWAN configuration in *SDWAN Configuration Guide*.

interface-id *interface-id*: Specifies an interface ID in the range of 1 to 255. For more information about interface ID, see SDWAN configuration in *SDWAN Configuration Guide*.

New command: qos lr outbound (user profile view)

Use **qos lr outbound** to configure traffic rate limiting settings for a user profile.

Use **undo qos lr outbound** to restore the default.

Syntax

```
qos lr outbound { cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] | peer-advertise-bandwidth }
```

```
undo qos lr outbound
```

Default

No traffic rate limiting settings are configured for a user profile.

Views

User profile view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Specifies the CIR in the range of 8 to 10000000 kbps.

cbs *committed-burst-size*: Specifies the CBS in the range of 1000 to 1000000000 bytes.

ebs *excess-burst-size*: Specifies the EBS in the range of 0 to 1000000000 bytes.

peer-advertise-bandwidth: Uses the CIR advertised by the peer tunnel interface. This CIR is configured by using the **qos bandwidth downstream** command on the peer tunnel interface and advertised during data channel establishment.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure traffic rate limiting settings based on user profile **a** and use the CIR configured by using the **qos bandwidth downstream** command on the peer tunnel interface.

```
<Sysname> system-view
[Sysname] user-profile a
[Sysname-user-profile-a] qos lr outbound peer-advertise-bandwidth
```

Configure traffic rate limiting settings based on user profile **a** and set the CIR to 1000 kbps.

```
<Sysname> system-view
[Sysname] user-profile a
[Sysname-user-profile-a] qos lr outbound cir 1000
```

Related commands

qos bandwidth downstream

New command: qos bandwidth downstream

Use **qos bandwidth downstream** to set the traffic rate limit to be applied to the outbound direction of the peer tunnel interface.

Use **undo qos bandwidth downstream** to restore the default.

Syntax

qos bandwidth downstream *bandwidth-value*

undo qos bandwidth downstream

Default

The traffic rate limit to be applied to the outbound direction of the peer tunnel interface is not configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies a bandwidth limit in the range of 8 to 10000000 kbps.

Usage guidelines

This command is applicable to only SDWAN tunnels. For more information about this feature, see SDWAN configuration in *SDWAN Configuration Guide*.

In the SDWAN scenario, a large number of spoke devices exist in a hub-spoke network. To configure a QoS policy for each hub-spoke SDWAN tunnel, you need to manually configure and apply a QoS policy on the hub device in the central site each time a spoke device is added for a branch site. If the QoS policies for the SDWAN tunnels from the central site to the branch sites are the same except for the rate limiting settings, you can simplify QoS policy configuration on the hub device by executing this command on the spoke devices.

The configuration procedure is as follows:

1. Execute the **qos apply user-profile downstream** command on the spoke device to apply the specified user profile to the hub-spoke SDWAN tunnel.
2. Execute the **qos bandwidth downstream** command on the spoke device to enable the BGP IPv4 Tnl-encap-ext routes to carry the specified traffic rate limit. The traffic rate limit will be advertised together with the TTE information to the hub device during hub-spoke SDWAN tunnel establishment.
3. Execute the **qos lr outbound** command with the **peer-advertise-bandwidth** keyword specified in the view of the user profile applied to the SDWAN tunnel. If you do not perform the above tasks on the peer hub device, the traffic rate limit specified by the **qos bandwidth downstream** command does not take effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the traffic rate limit to be applied to the outbound direction of the peer tunnel interface to 1000 kbps.

```
<Sysname> system-view
[Sysname] interface Tunnel 2 mode sdwan udp
[Sysname-Tunnel2] qos bandwidth downstream 1000
```

Related commands

- **qos apply user-profile downstream**
- **qos lr outbound** (user profile view)

New command: qos pq (user profile view)

Use **qos pq** to apply a PQ list to a user profile.

Use **undo qos pq** to restore the default.

Syntax

qos pq pql *pql-index*

undo qos pq

Default

No PQ list is applied to a user profile.

Views

User profile view

Predefined user roles

network-admin

Parameters

pql-index: Specifies a PQ list by its number in the range of 1 to 16.

Usage guidelines

PQ is designed for mission-critical applications. Mission-critical applications require preferential treatment to reduce the response delay when congestion occurs. PQ can flexibly determine the order of forwarding packets by network protocol (for example, IP and IPX), incoming interface, packet length, and source/destination address.

You can execute this command to apply a user profile with a PQ list configured to different interfaces, without configuring the PQ list for each interface.

For a user profile, if you execute this command multiple times, the most recent configuration takes effect.

You can define a set of assignment rules in a PQ list. When a packet arrives, it is examined against match criteria in their configuration order.

- When a match is found, the packet is assigned to the corresponding queue, and the matching process ends.
- If no match is found, the packet is assigned to the default queue.

Examples

```
# Apply PQ list 12 to user profile a.
<Sysname> system-view
[Sysname] user-profile a
[Sysname-user-profile-a] qos pq pql 12
```

New feature: Configuring interface channelization

Configuring interface channelization

About this task

By default, all subinterfaces of a main interface share and contend for the bandwidth of the main interface. Subinterfaces that carry key services cannot be guaranteed enough bandwidth. This feature allows subinterfaces of a physical interface or aggregate interface to exclusively use the specified amount of bandwidth.

Procedure

1. Enter system view.
system-view
2. Enter subinterface view.
interface *interface-type interface-number.subnumber*
3. Set the channelized bandwidth for the subinterface.
mode channel-bandwidth *bandwidth-value*

By default, the channelized bandwidth is not set for a subinterface.

Command reference

New command: display mode channel-bandwidth interface

Use **display mode channel-bandwidth interface** to display interface channelization configuration and statistics.

Syntax

In standalone mode:

```
display mode channel-bandwidth interface [ interface-type { interface-number | interface-number.subnumber } ]
```

In IRF mode:

```
display mode channel-bandwidth interface [ interface-type { interface-number | interface-number.subnumber } ] [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type: Specifies an interface type. If you do not specify an interface, this command displays the interface channelization configuration for all subinterfaces.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument represents the number of the main interface.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the interface channelization configuration for all member devices. (In IRF mode.)

Examples

Display the interface channelization configuration for GigabitEthernet 1/0/1.1.

```
<Sysname> display mode channel-bandwidth interface gigabitethernet 1/0/1.1
Subinterface : GE1/0/1.1                Channelized bandwidth : 100 kbps
  Passed      : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed    : 1000 (Packets) 1000 (Bytes)
```

Display the interface channelization configuration for all interfaces.

```
<Sysname> display mode channel-bandwidth interface
Interface : GE1/0/1                Total bandwidth      : 1000000 kbps
Total channelized bandwidth : 600 kbps
Subinterface : GE1/0/1.1          Channelized bandwidth : 100 kbps
  Passed      : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed    : 1000 (Packets) 1000 (Bytes)
Subinterface : GE1/0/1.2          Channelized bandwidth : 200 kbps
  Passed      : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed    : 1000 (Packets) 1000 (Bytes)
Subinterface : GE1/0/1.3          Channelized bandwidth : 300 kbps
  Passed      : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed    : 1000 (Packets) 1000 (Bytes)

Interface : GE1/0/2                Total bandwidth      : 1000000 kbps
Total channelized bandwidth : 600 kbps
Subinterface : GE1/0/2.1          Channelized bandwidth : 100 kbps
  Passed      : 1000 (Packets) 1000 (Bytes)
```

```

Discarded: 1000 (Packets) 1000 (Bytes)
Delayed   : 1000 (Packets) 1000 (Bytes)
Subinterface : GE1/0/2.2           Channelized bandwidth : 200 kbps
Passed    : 1000 (Packets) 1000 (Bytes)
Discarded: 1000 (Packets) 1000 (Bytes)
Delayed   : 1000 (Packets) 1000 (Bytes)
Subinterface : GE1/0/2.3           Channelized bandwidth : 300 kbps
Passed    : 1000 (Packets) 1000 (Bytes)
Discarded: 1000 (Packets) 1000 (Bytes)
Delayed   : 1000 (Packets) 1000 (Bytes)
...

```

Table 6 Command output

Field	Description
Slot	Number of the slot where the aggregate interface resides.
Interface	Main interface.
Total bandwidth	Total bandwidth of the main interface.
Total channelized bandwidth	Total channelized bandwidth of all subinterfaces configured.
Passed	Number and bytes of packets that have been forwarded.
Discarded	Number and bytes of dropped packets.
Passed	Number and bytes of packets that have been forwarded.
Field	Description

Related commands

mode channel-bandwidth

New command: mode channel-bandwidth

Use **mode channel-bandwidth** to set the channelized bandwidth for a subinterface.

Use **undo mode channel-bandwidth** to restore the default.

Syntax

mode channel-bandwidth *bandwidth-value*

undo mode channel-bandwidth

Default

The channelized bandwidth is not set for a subinterface.

Views

Subinterface view

Predefined user roles

network-admin

Parameters

bandwidth-value: Specifies the channelized bandwidth in the range of 30 to 9500000 kbps.

Usage guidelines

By default, all subinterfaces of a main interface share and contend for the bandwidth of the main interface. Subinterfaces that carry key services cannot be guaranteed enough bandwidth. This feature allows subinterfaces of a physical interface or aggregate interface to exclusively use the specified amount of bandwidth.

Before configuring the channelized bandwidth for a Layer 3 aggregate subinterface, you must execute the **bandwidth** command on the aggregate interface.

The total channelized bandwidth of subinterfaces cannot exceed the actual bandwidth of the main interface plus 1 Mbps. The channelized bandwidth takes effect only in the outbound direction.

Examples

```
# Set the channelized bandwidth to 100 kbps for GigabitEthernet 1/0/1.1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1.1
```

```
[Sysname-GigabitEthernet1/0/1.1] mode channel-bandwidth 100
```

Related commands

bandwidth (*Layer 2—LAN Switching Command Reference*)

display mode channel-bandwidth interface

New feature: Configuring a default color value for public network and L3VPN route recursion to an SRv6 TE policy

Configure a default color value for public network and VPN route recursion to an SRv6 TE policy

About this task

The local PE uses the default color value to match an SRv6 TE policy for a received public network or VPN route if the route does not carry a color extended community and no color is added to the route through a routing policy.

Configuring a default color value for VPN routes

1. Enter system view.
system-view
2. Enter VPN instance view.
ip vpn-instance *vpn-instance-name*
3. Enter IPv4 address family view or IPv6 address family view of the VPN instance.
 - Enter VPN instance IPv4 address family view.
address-family ipv4
 - Enter VPN instance IPv6 address family view.
address-family ipv6
4. Configure a default color value for L3VPN route recursion to an SRv6 TE policy.
default-color *color-value* [**evpn**]

By default, no default color is configured for L3VPN route recursion to an SRv6 TE policy.

Configuring a default color value for public network routes

1. Enter system view.
system-view
2. Enter public instance view.
ip public-instance
3. Enter public instance IPv4 or IPv6 address family view.
 - o Enter public instance IPv4 address family view
address-family ipv4
 - o Enter public instance IPv6 address family view.
address-family ipv6
4. Configure a default color value for public network route recursion to an SRv6 TE policy.
default-color color-value

By default, no default color value is configured for public network route recursion to an SRv6 TE policy.

Command reference

default-color (public instance IPv4/IPv6 address family view)

Use **default-color** to configure a default color value for public route recursion to an SRv6 TE policy.

Use **undo default-color** to restore the default.

Syntax

default-color color-value

undo default-color

Default

No default color value is configured.

Views

Public instance IPv4 address family view

Public instance IPv6 address family view

Predefined user roles

network-admin

Parameters

color-value: Default color value in the range of 0 to 4294967295.

Usage guidelines

The local PE uses the default color value to match an SRv6 TE policy for a received public network route if the route does not carry a color extended community and no color is added to the route through a routing policy.

This command applies only to the public network routes learned from a remote PE.

The default color value configured by this command is used only for SRv6 TE policy traffic steering. It does not used in route advertisement.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In public instance IPv4 address family view, set the default color to 100 for public network route recursion to an SRv6 TE policy.

```
<Sysname> system-view
[Sysname] ip public-instance
[Sysname-public-instance] address-family ipv4
[Sysname-public-instance-ipv4] default-color 100
```

default-color (VPN instance IPv4/IPv6 address family view)

Use **default-color** to configure a default color value for L3VPN route recursion to an SRv6 TE policy.

Use **undo default-color** to restore the default.

Syntax

default-color *color-value* [**evpn**]

undo default-color [**evpn**]

Default

No default color value is configured.

Views

VPN instance IPv4 address family view

VPN instance IPv6 address family view

Predefined user roles

network-admin

Parameters

color-value: Default color value in the range of 0 to 4294967295.

evpn: Specifies the EVPN L3VPN service. If you do not specify this keyword, the default color applies to MPLS L3VPN route recursion to an SRv6 TE policy.

Usage guidelines

The local PE uses the default color value to match an SRv6 TE policy for a received VPNv4, VPNv6, or EVPN IP prefix route if the route does not carry a color extended community and no color is added to the route through a routing policy.

This command applies only to the VPN routes learned from a remote PE.

The default color value configured by this command is used only for SRv6 TE policy traffic steering. It does not used in route advertisement.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In IPv4 address family view for VPN instance **vpn1**, set the default color to 100 for EVPN L3VPN route recursion to an SRv6 TE policy.

```
<Sysname> system-view
```

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] address-family ipv4
[Sysname-vpn-instance-vpn1] default-color 100 evpn
```

New feature: SRv6 TE policy route recursion support for SRv6-TE and SRv6-BE FRR mode

Configuring SRv6-TE and SRv6-BE FRR mode

About this task

Public network IP over SRv6, EVPN L3VPN over SRv6, and IP L3VPN over SRv6 support the following route recursion modes:

- SRv6-BE mode.
- SRv6-TE mode.
- SRv6-TE and SRv6-BE hybrid mode.
- SRv6-TE and SRv6-BE FRR mode.

As from this release, the device adds support for the SRv6-TE and SRv6-BE FRR mode.

Procedure

1. Enter system view.

system-view

2. Enter BGP instance view.

bgp as-number [instance instance-name]

3. Enter BGP-VPN instance view.

ip vpn-instance vpn-instance-name

4. Enter BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view.

- Enter BGP-VPN IPv4 unicast address family view.

address-family ipv4 [unicast]

- Enter BGP-VPN IPv6 unicast address family view.

address-family ipv6 [unicast]

5. Configure the route recursion mode.

segment-routing ipv6 { best-effort | traffic-engineer | traffic-engineer best-effort | traffic-engineer best-effort-backup }

By default, a PE searches the IPv6 routing table based on the next hop of a matching route to forward traffic.

If multiple SRv6-BE paths exist among the source and destination nodes in an SRv6 TE policy, the SRv6-BE path with the lowest next hop address is selected as the backup path.

Command reference

Modified command: segment-routing ipv6 traffic-engineering

Use **segment-routing ipv6 traffic-engineering** to recurse routes to SRv6 TE policy tunnels.

Use **undo segment-routing ipv6 traffic-engineering** to restore the default.

Old syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort**] [**evpn**]

undo segment-routing ipv6 traffic-engineering [**best-effort**] [**evpn**]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 traffic-engineering [**best-effort**]

undo segment-routing ipv6 traffic-engineering [**best-effort**]

In BGP EVPN address family view:

segment-routing ipv6 traffic-engineering [**best-effort**] **evpn**

undo segment-routing ipv6 traffic-engineering [**best-effort**] **evpn**

In BGP IPv4 unicast address family view or BGP IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort**]

undo segment-routing ipv6 traffic-engineering [**best-effort**]

New syntax

In BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**] [**evpn**]

undo segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**] [**evpn**]

In BGP VPNv4 address family view or BGP VPNv6 address family view:

segment-routing ipv6 traffic-engineering [**best-effort**]

undo segment-routing ipv6 traffic-engineering [**best-effort**]

In BGP EVPN address family view:

segment-routing ipv6 traffic-engineering [**best-effort**] **evpn**

undo segment-routing ipv6 traffic-engineering [**best-effort**] **evpn**

In BGP IPv4 unicast address family view or BGP IPv6 unicast address family view:

segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**]

undo segment-routing ipv6 traffic-engineering [**best-effort** | **best-effort-backup**]

Views

BGP-VPN IPv4 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP IPv4 unicast address family view
BGP IPv6 unicast address family view
BGP VPNv4 address family view
BGP VPNv6 address family view
BGP EVPN address family view

Change description

The **best-effort-backup** keyword was added.

best-effort-backup: Implements FRR by using the SRv6-TE path (primary path) and SRv6-BE path (backup path). If the SRv6-TE path fails or does not exist, traffic is immediately switched to the SRv6-BE path to ensure service continuity. If multiple SRv6-BE paths exist between the source and destination nodes, the SRv6-BE path with the lowest next hop address is selected as the backup path.

New feature: Configuring the SRv6 TE policy encapsulation mode

Configuring the SRv6 TE policy encapsulation mode

About this task

If the traffic steering mode is BSID, packets whose destination IPv6 address is the same as the BSID of an SRv6 TE policy will be forwarded by the SRv6 TE policy. In this case, the device needs to encapsulate the SID list of the SRv6 TE policy into the packets. The following encapsulation modes are available:

- **Encaps**—Normal encapsulation mode. It adds a new IPv6 header and an SRH to the original packets. All SIDs in the SID list of the SRv6 TE policy are encapsulated in the SRH.
- **Encaps.Red**—Reduced mode of normal encapsulation. It adds a new IPv6 header and an SRH to the original packets. The first SID in the SID list of the SRv6 TE policy is not encapsulated in the SRH to reduce the SRH length. All other SIDs in the SID list are encapsulated in the SRH.
- **Insert**—Insertion mode. It inserts an SRH after the original IPv6 header. All SIDs in the SID list of the SRv6 TE policy are encapsulated in the SRH.
- **Insert.Red**—Reduced insertion mode. It inserts an SRH after the original IPv6 header. The first SID in the SID list of the SRv6 TE policy is not encapsulated in the SRH to reduce the SRH length. All other SIDs in the SID list are encapsulated in the SRH.

In **Encaps** or **Encaps.Red** encapsulation mode, the destination IPv6 address in the new IPv6 header is the first SID in the SID list of the SRv6 TE policy. The source IPv6 address is the IPv6 address specified by using the **encapsulation source-address** command.

In **Insert** or **Insert.Red** encapsulation mode, the destination IPv6 address in the original IPv6 header is changed to the first SID in the SID list of the SRv6 TE policy. The source IPv6 address in the original IPv6 header does not change.

If the traffic steering mode is BSID and the SRv6 SID of the ingress node is an End.X SID, the device does not encapsulate the End.X SID into the SRH by default.

To obtain complete SRv6 forwarding path information from the SRH of packets, you can configure the device to encapsulate the local End.X SID in the SRH.

Restrictions and guidelines

You can configure the encapsulation mode for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence

over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

The normal encapsulation modes are exclusive with the insertion modes. If you configure both a normal encapsulation mode and an insertion mode for an SRv6 TE policy, the most recent configuration takes effect.

If you configure the **Insert** or **Insert.Red** mode for an SRv6 TE policy, it uses the **Encaps** mode to encapsulate received IPv4 packets.

In SRv6 TE view, if you execute both the **srv6-policy encapsulation-mode encaps reduced** command and the **srv6-policy encapsulation-mode encaps include local-end.x** command, the **srv6-policy encapsulation-mode encaps include local-end.x** command takes effect.

In SRv6 TE view, if you execute both the **srv6-policy encapsulation-mode insert reduced** command and the **srv6-policy encapsulation-mode insert include local-end.x** command, the **srv6-policy encapsulation-mode insert include local-end.x** command takes effect.

In SRv6 TE policy view, if you execute both the **encapsulation-mode encaps reduced** command and the **encapsulation-mode encaps include local-end.x** command, the **encapsulation-mode encaps include local-end.x** command takes effect.

In SRv6 TE policy view, if you execute both the **encapsulation-mode insert reduced** command and the **encapsulation-mode insert include local-end.x** command, the **encapsulation-mode insert include local-end.x** command takes effect.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 TE view.
traffic-engineering
4. Configure the encapsulation mode globally for all SRv6 TE policies. Choose one option as needed:
 - Specify the Encaps.Red encapsulation mode globally for all SRv6 TE policies.
srv6-policy encapsulation-mode encaps reduced
 - Specify the Insert or Insert.Red encapsulation mode globally for all SRv6 TE policies.
srv6-policy encapsulation-mode insert
srv6-policy encapsulation-mode insert reduced

By default, an SRv6 TE policy uses the Encaps encapsulation mode.
5. Enable the device to include the local End.X SID in the SRH of the packets forwarded by SRv6 TE policies. Choose one option as needed:
 - Enable this feature for SRv6 TE policies with a normal encapsulation mode
srv6-policy encapsulation-mode encaps include local-end.x
 - Enable this feature for SRv6 TE policies with an insertion encapsulation mode
srv6-policy encapsulation-mode insert include local-end.x

By default, the device does not include the local End.X SID in the SRH of the packets forwarded by SRv6 TE policies.
6. Enter SRv6 TE policy view.
policy policy-name
7. Configure the encapsulation mode for the SRv6 TE policy. Choose one option as needed:
 - Specify the Encaps.Red encapsulation mode for the SRv6 TE policy.

encapsulation-mode encaps reduced [disable]

- Specify the Insert or Insert.Red encapsulation mode globally for all SRv6 TE policies.

encapsulation-mode insert

encapsulation-mode insert reduced [disable]

By default, the encapsulation mode is not configured for an SRv6 TE policy, and the encapsulation mode configured in SRv6 TE view applies.

8. Configure local End.X SID encapsulation in the SRH of the packets forwarded by the SRv6 TE policy.

- Configure this feature when the SRv6 TE policy uses a normal encapsulation mode.

encapsulation-mode encaps include local-end.x [disable]

- Configure this feature when the SRv6 TE policy uses an insertion encapsulation mode.

encapsulation-mode insert include local-end.x [disable]

By default, local End.X SID encapsulation is not configured for an SRv6 TE policy, and the local End.X SID encapsulation setting configured in SRv6 TE view applies.

Command reference

New command: encapsulation-mode

Use **encapsulation-mode** to configure the encapsulation mode for an SRv6 TE policy.

Use **undo encapsulation-mode** to restore the default.

Syntax

encapsulation-mode encaps reduced [disable]

undo encapsulation-mode encaps reduced

encapsulation-mode insert

undo encapsulation-mode insert

encapsulation-mode insert reduced [disable]

undo encapsulation-mode insert reduced

Default

The encapsulation mode is not configured for an SRv6 TE policy, and the encapsulation mode configured in SRv6 TE view applies.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

encaps reduced: Specifies the encapsulation mode as reduced encapsulation mode.

insert: Specifies the encapsulation mode as insertion mode.

insert reduced: Specifies the encapsulation mode as reduced insertion mode.

disable: Disables the specified encapsulation mode.

Usage guidelines

If the traffic steering mode is BSID, packets whose destination IPv6 address is the same as the BSID of an SRv6 TE policy will be forwarded by the SRv6 TE policy. In this case, the device needs to encapsulate the SID list of the SRv6 TE policy into the packets. The following encapsulation modes are available:

- **Encaps**—Normal encapsulation mode. It adds a new IPv6 header and an SRH to the original packets. All SIDs in the SID list of the SRv6 TE policy are encapsulated in the SRH.
- **Encaps.Red**—Reduced mode of the normal encapsulation mode. It adds a new IPv6 header and an SRH to the original packets. The first SID in the SID list of the SRv6 TE policy is not encapsulated in the SRH to reduce the SRH length. All other SIDs in the SID list are encapsulated in the SRH.
- **Insert**—Insertion mode. It inserts an SRH after the original IPv6 header. All SIDs in the SID list of the SRv6 TE policy are encapsulated in the SRH.
- **Insert.Red**—Reduced insertion mode. It inserts an SRH after the original IPv6 header. The first SID in the SID list of the SRv6 TE policy is not encapsulated in the SRH to reduce the SRH length. All other SIDs in the SID list are encapsulated in the SRH.

In **Encaps** or **Encaps.Red** encapsulation mode, the destination IPv6 address in the new IPv6 header is the first SID in the SID list of the SRv6 TE policy. The source IPv6 address is the IPv6 address specified by using the **encapsulation source-address** command.

In **Insert** or **Insert.Red** encapsulation mode, the destination IPv6 address in the original IPv6 header is changed to the first SID in the SID list of the SRv6 TE policy. The source IPv6 address in the original IPv6 header does not change.

You can configure the encapsulation mode for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

The normal encapsulation modes are exclusive with the insertion modes. If you configure a normal encapsulation mode and an insertion mode for an SRv6 TE policy, the most recent configuration takes effect.

If you configure the **Insert** or **Insert.Red** mode for an SRv6 TE policy, it uses the **Encaps** mode to encapsulate received IPv4 packets.

If you execute both the **encapsulation-mode encaps reduced** command and the **encapsulation-mode encaps include local-end.x** command for an SRv6 TE policy, the **encapsulation-mode encaps include local-end.x** command takes effect.

If you execute both the **encapsulation-mode insert reduced** command and the **encapsulation-mode insert include local-end.x** command for an SRv6 TE policy, the **encapsulation-mode insert include local-end.x** command takes effect.

Examples

Configure SRv6 TE policy 1 to use the Encaps.Red encapsulation.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy 1
[Sysname-srv6-te-policy-1] encapsulation-mode encaps reduced
```

Related commands

encapsulation source-address

srv6-policy encapsulation-mode

New command: encapsulation-mode encaps include local-end.x

Use **encapsulation-mode encaps include local-end.x** to configure local End.X SID encapsulation in the SRH of the packets forwarded by an SRv6 TE policy with a normal encapsulation mode.

Use **undo encapsulation-mode encaps include local-end.x** to restore the default.

Syntax

encapsulation-mode encaps include local-end.x [disable]

undo encapsulation-mode encaps include local-end.x

Default

The local End.X SID encapsulation is not configured for an SRv6 TE policy with a normal encapsulation mode, and the local End.X SID encapsulation setting configured in SRv6 TE view applies.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

disable: Disables encapsulating the local End.X SID into the SRH header of packets forwarded by an SRv6 TE policy with a normal encapsulation mode. If you do not specify this keyword, the local End.X SID will be encapsulated into the SRH of the packets.

Usage guidelines

If the traffic steering mode is BSID and the SRv6 SID of the ingress node is an End.X SID, the device does not encapsulate the End.X SID into the SRH by default.

To obtain complete SRv6 forwarding path information from the SRH of packets, use this command to configure the device to encapsulate the local End.X SID in the SRH.

You can configure the local End.X SID encapsulation for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

If you execute the **encapsulation-mode encaps include local-end.x** command and the **encapsulation-mode insert include local-end.x** command for an SRv6 TE policy, the most recent configuration takes effect.

If you execute both the **encapsulation-mode encaps reduced** command and the **encapsulation-mode encaps include local-end.x** command for an SRv6 TE policy, the **encapsulation-mode encaps include local-end.x** command takes effect.

Examples

Include the End.X SID in the SRH of the packets forwarded by an SRv6 TE policy with a normal encapsulation mode.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy 1
[Sysname-srv6-te-policy-1] encapsulation-mode encaps include local-end.x
```

Related commands

srv6-policy encapsulation-mode encaps include local-end.x

New command: encapsulation-mode insert include local-end.x

Use **encapsulation-mode insert include local-end.x** to configure local End.X SID encapsulation in the SRH of the packets forwarded by an SRv6 TE policy with an insertion encapsulation mode.

Use **undo encapsulation-mode insert include local-end.x** to restore the default.

Syntax

encapsulation-mode insert include local-end.x [disable]

undo encapsulation-mode insert include local-end.x

Default

The local End.X SID encapsulation is not configured for an SRv6 TE policy with an insertion encapsulation mode, and the local End.X SID encapsulation setting configured in SRv6 TE view applies.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

disable: Disables encapsulating the local End.X SID into the SRH header inserted into the packets forwarded by an SRv6 TE policy with an insertion encapsulation mode. If you do not specify this keyword, the local End.X SID will be encapsulated into the SRH of the packets.

Usage guidelines

If the traffic steering mode is BSID and the SRv6 SID of the ingress node is an End.X SID, the device does not encapsulate the End.X SID into the SRH by default.

To obtain complete SRv6 forwarding path information from the SRH of packets, use this command to configure the device to encapsulate the local End.X SID in the SRH.

You can configure the local End.X SID encapsulation for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

If you execute the **encapsulation-mode encaps include local-end.x** command and the **encapsulation-mode insert include local-end.x** command alternately for an SRv6 TE policy, the most recent configuration takes effect.

If you execute both the **encapsulation-mode insert reduced** command and the **encapsulation-mode insert include local-end.x** command for an SRv6 TE policy, the **encapsulation-mode insert include local-end.x** command takes effect.

Examples

Include the End.X SID in the SRH of the packets forwarded by an SRv6 TE policy with an insertion encapsulation mode.

```
<Sysname> system-view
```

```
[Sysname] segment-routing ipv6
```

```
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy 1
[Sysname-srv6-te-policy-1] encapsulation-mode insert include local-end.x
```

Related commands

srv6-policy encapsulation-mode insert include local-end.x

New command: srv6-policy encapsulation-mode

Use **srv6-policy encapsulation-mode** to enable the reduced encapsulation mode for all SRv6 TE policies globally.

Use **undo srv6-policy encapsulation-mode** to restore the default.

Syntax

```
srv6-policy encapsulation-mode encaps reduced
undo srv6-policy encapsulation-mode encaps reduced
srv6-policy encapsulation-mode insert
undo srv6-policy encapsulation-mode insert
srv6-policy encapsulation-mode insert reduced
undo srv6-policy encapsulation-mode insert reduced
```

Default

An SRv6 TE policy uses the normal encapsulation (Encaps) mode.

Views

SRv6 TE view

Predefined user roles

network-admin

Parameters

encaps reduced: Specifies the encapsulation mode as reduced encapsulation mode.

insert: Specifies the encapsulation mode as insertion mode.

insert reduced: Specifies the encapsulation mode as reduced insertion mode.

Usage guidelines

If the traffic steering mode is BSID, packets whose destination IPv6 address is the same as the BSID of an SRv6 TE policy will be forwarded by the SRv6 TE policy. In this case, the device needs to encapsulate the SID list of the SRv6 TE policy into the packets. The following encapsulation modes are available:

- **Encaps**—Normal encapsulation mode. It adds a new IPv6 header and an SRH to the original packets. All SIDs in the SID list of the SRv6 TE policy are encapsulated in the SRH.
- **Encaps.Red**—Reduced mode of the normal encapsulation mode. It adds a new IPv6 header and an SRH to the original packets. The first SID in the SID list of the SRv6 TE policy is not encapsulated in the SRH to reduce the SRH length. All other SIDs in the SID list are encapsulated in the SRH.
- **Insert**—Insertion mode. It inserts an SRH after the original IPv6 header. All SIDs in the SID list of the SRv6 TE policy are encapsulated in the SRH.
- **Insert.Red**—Reduced insertion mode. It inserts an SRH after the original IPv6 header. The first SID in the SID list of the SRv6 TE policy is not encapsulated in the SRH to reduce the SRH length. All other SIDs in the SID list are encapsulated in the SRH.

In **Encaps** or **Encaps.Red** encapsulation mode, the destination IPv6 address in the new IPv6 header is the first SID in the SID list of the SRv6 TE policy. The source IPv6 address is the IPv6 address specified by using the **encapsulation source-address** command.

In **Insert** or **Insert.Red** encapsulation mode, the destination IPv6 address in the original IPv6 header is changed to the first SID in the SID list of the SRv6 TE policy. The source IPv6 address in the original IPv6 header is not changed.

You can configure the encapsulation mode for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

The normal encapsulation modes are exclusive with the insertion modes. If you configure a normal encapsulation mode and an insertion mode alternately, the most recent configuration takes effect.

If you configure the **Insert** or **Insert.Red** mode for an SRv6 TE policy, it uses the **Encaps** mode to encapsulate received IPv4 packets.

If you execute both the **srv6-policy encapsulation-mode encaps reduced** command and the **srv6-policy encapsulation-mode encaps include local-end.x** command, the **srv6-policy encapsulation-mode encaps include local-end.x** command takes effect.

If you execute both the **srv6-policy encapsulation-mode insert reduced** command and the **srv6-policy encapsulation-mode insert include local-end.x** command, the **srv6-policy encapsulation-mode insert include local-end.x** command takes effect.

Examples

```
# Configure the Encaps.Red mode for all SRv6 TE policies globally.
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] srv6-policy encapsulation-mode encaps reduced
```

Related commands

encapsulation source-address

encapsulation-mode

New command: srv6-policy encapsulation-mode encaps include local-end.x

Use **srv6-policy encapsulation-mode encaps include local-end.x** to configure local End.X SID encapsulation for all SRv6 TE policies using a normal encapsulation mode.

Use **undo srv6-policy encapsulation-mode encaps include local-end.x** to restore the default.

Syntax

srv6-policy encapsulation-mode encaps include local-end.x

undo srv6-policy encapsulation-mode encaps include local-end.x

Default

The device does not encapsulate the local End.X SID into the SRH of the packets forwarded by an SRv6 TE policy using a normal encapsulation mode.

Views

SRv6 TE view

Predefined user roles

network-admin

Usage guidelines

If the traffic steering mode is BSID and the SRv6 SID of the ingress node is an End.X SID, the device does not encapsulate the End.X SID into the SRH by default.

To obtain complete SRv6 forwarding path information from the SRH of packets, use this command to configure the device to encapsulate the local End.X SID into the SRH.

You can configure the local End.X SID encapsulation for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

If you execute the **srv6-policy encapsulation-mode encaps include local-end.x** command and the **srv6-policy encapsulation-mode insert include local-end.x** command, the most recent configuration takes effect.

If you execute both the **srv6-policy encapsulation-mode encaps reduced** command and the **srv6-policy encapsulation-mode encaps include local-end.x** command, the **srv6-policy encapsulation-mode encaps include local-end.x** command takes effect.

Examples

Configure the device to include the local End.X SID in the SRH of the packets forwarded by SRv6 TE policies using a normal encapsulation mode.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] srv6-policy encapsulation-mode encaps include local-end.x
```

Related commands

encapsulation-mode encaps include local-end.x

New command: srv6-policy encapsulation-mode insert include local-end.x

Use **srv6-policy encapsulation-mode insert include local-end.x** to configure local End.X SID encapsulation for all SRv6 TE policies with an insertion encapsulation mode.

Use **undo srv6-policy encapsulation-mode insert include local-end.x** to restore the default.

Syntax

srv6-policy encapsulation-mode insert include local-end.x

undo srv6-policy encapsulation-mode insert include local-end.x

Default

The device does not encapsulate the local End.X SID into the SRH of the packets forwarded by an SRv6 TE policy with an insertion encapsulation mode.

Views

SRv6 TE view

Predefined user roles

network-admin

Usage guidelines

If the traffic steering mode is BSID and the SRv6 SID of the ingress node is an End.X SID, the device does not encapsulate the End.X SID into the SRH by default.

To obtain complete SRv6 forwarding path information from the SRH of packets, use this command to configure the device to encapsulate the local End.X SID into the SRH.

You can configure the local End.X SID encapsulation for all SRv6 TE policies globally in SRv6 TE view or for a specific SRv6 TE policy in SRv6 TE policy view. The policy-specific configuration takes precedence over the global configuration. An SRv6 TE policy uses the global configuration only when it has no policy-specific configuration.

If you execute the **srv6-policy encapsulation-mode encaps include local-end.x** command and the **srv6-policy encapsulation-mode insert include local-end.x** command multiple times, the most recent configuration takes effect.

If you execute both the **srv6-policy encapsulation-mode insert reduced** command and the **srv6-policy encapsulation-mode insert include local-end.x** command, the **srv6-policy encapsulation-mode insert include local-end.x** command takes effect.

Examples

Enable the device to include the local End.X SID in the SRH of the packets forwarded by SRv6 TE policies with an insertion encapsulation mode.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] srv6-policy encapsulation-mode insert include local-end.x
```

Related commands

encapsulation-mode insert include local-end.x

Modified command: display segment-routing ipv6 local-sid

Use **display segment-routing ipv6 local-sid** to display information about the SRv6 local SID forwarding table.

Old syntax

```
display segment-routing ipv6 local-sid { end | end-am | end-as | end-b6encaps |
end-coc32 | end-dt2m | end-dt2u | end-dt2ul | end-dx2 | end-dx2l | end-m | end-op |
end-t | end-x-coc32 } [ sid ]
```

```
display segment-routing ipv6 local-sid { end-dt4 | end-dt46 | end-dt6 | end-dx4 |
end-dx6 } [ sid | vpn-instance vpn-instance-name ]
```

```
display segment-routing ipv6 local-sid end-x [ sid | interface interface-type
interface-number [ nexthop nexthop-ipv6-address ] ]
```

New syntax

```
display segment-routing ipv6 local-sid { end | end-am | end-as | end-b6encaps |
end-b6encapsred | end-b6insert | end-b6insertred | end-coc32 | end-dt2m | end-dt2u
| end-dt2ul | end-dx2 | end-dx2l | end-m | end-op | end-t | end-x-coc32 } [ sid ]
```

```
display segment-routing ipv6 local-sid { end-dt4 | end-dt46 | end-dt6 | end-dx4 |
end-dx6 } [ sid | vpn-instance vpn-instance-name ]
```

```
display segment-routing ipv6 local-sid end-x [ sid | interface interface-type  
interface-number [ nexthop nexthop-ipv6-address ] ]
```

Views

Any view

Change description

The following keywords were added:

- **end-b6encapsred**: Specifies End.B6ENCAPSRED SIDs.
- **end-b6insert**: Specifies End.B6INSERT SIDs.
- **end-b6insertred**: Specifies End.B6INSERTRED SIDs.

New feature: Configuring the Next Header field value in the SRH of SRv6 packets

Configuring the Next Header field value in the SRH of SRv6 packets

About this task

In an EVPN VPWS over SRv6 network or an EVPN VPLS over SRv6 network, the device validates the Next Header field in the SRH of SRv6 packets. If the validation fails, the device processes the SRv6 packets as normal packets, which might result in packet loss. To ensure correct processing of SRv6 packets containing incompatible versions, you can perform this task to edit the Next Header field value in the SRH of the SRv6 packets.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Configure the Next Header field value in the SRH of SRv6 packets.
evpn next-header-field { 59 | 143 }

By default, the Next Header field value in the SRH is 143.

Command reference

evpn next-header-field

Use **evpn next-header-field** to configure the value of the Next Header field in the SRH.

Use **undo evpn next-header-field** to restore the default.

Syntax

evpn next-header-field { 59 | 143 }

undo evpn next-header-field

Default

The value of the Next Header field in the SRH is 143.

Views

SRv6 view

Predefined user roles

network-admin

Parameters

59: Sets the value of the Next Header field in the SRH to 59.

143: Sets the value of the Next Header field in the SRH to 143.

Usage guidelines

On EVPN VPWS over SRv6 and EVPN VPLS over SRv6 networks, the device identifies SRv6 packets by the value of the Next Header field in the SRH. If the value in a packet is different from that set on the device, the device processes the packet as a normal IPv6 packet rather than an SRv6 packet. For the device to successfully identify SRv6 packets, you can change the value on the device according to the value supported by the peer device.

Examples

```
# Set the value of the Next Header field in the SRH to 59.
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] evpn next-header-field 59
```

New feature: SRv6 TE policy rate limit

Configuring a rate limit for an SRv6 TE policy

About this task

When the rate of the packets forwarded by an SRv6 TE policy exceeds the rate limit, the device drops the packets that exceed the rate limit.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 TE view.
traffic-engineering
4. Enter SRv6 TE policy view.
policy *policy-name*
5. Set a rate limit for the SRv6 TE policy.
rate-limit *kbps*
By default, no rate limit is set for an SRv6 TE policy.

Command reference

rate-limit

Use **rate-limit** to set a rate limit for an SRv6 TE policy.

Use **undo rate-limit** to restore the default.

Syntax

rate-limit *kbps*

undo rate-limit

Default

No rate limit is set for an SRv6 TE policy.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

kbps: Specifies the rate limit, in the range of 1 to 4294967295, in kbps.

Usage guidelines

When the rate of the packets forwarded by an SRv6 TE policy exceeds the rate limit, the device drops the packets that exceed the rate limit.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the rate limit for SRv6 TE policy **aaa** to 15000 kbps.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy aaa
[Sysname-srv6-te-policy-aaa] rate-limit 15000
```

New feature: Configuring next hop-based dynamic End.DX4 or End.DX6 SID allocation for public or private network routes

Configuring next hop-based dynamic End.DX4 or End.DX6 SID allocation for public or private network routes

About this task

This task is applicable to the IP L3VPN over SRv6 and public network IP over SRv6 scenarios.

- In the IP L3VPN over SRv6 scenario:

Perform this task to forward an SRv6 decapsulated VPN packet to the next hop without looking up the routing table of the VPN instance.

By default, all BGP private network routes of a VPN instance are allocated the SID of the VPN instance. When a PE removes the SRv6 encapsulation from a received packet, it looks up the routing table of the VPN instance based on the SID for an optimal route. Then, the PE forwards the packet to a CE. To forward the packet to the next hop without looking up the routing table of the VPN instance, perform this task.

This task dynamically allocates End.DX4 or End.DX6 SIDs to all next hops of the BGP private network routes in a VPN instance based on the next hop addresses. When forwarding a packet, the PE searches for the output interface and next hop based on the End.DX4 or End.DX6 SID of the packet. Then, the PE directly forwards the packet out of the output interface to the next hop.

- In the public network IP over SRv6 scenario:

By default, a PE allocates the same SID to all BGP public network routes. When the PE removes the SRv6 encapsulation from a received packet, it looks up the routing table of the public network based on the SID for an optimal route. To forward the packet to the next hop without looking up the routing table, configure this feature.

This feature dynamically allocates End.DX4 or End.DX6 SIDs to all next hops for the BGP public network routes. When forwarding a packet, the PE searches for the output interface and next hop based on the End.DX4 or End.DX6 SID of the packet. Then, the PE directly forwards the packet out of the output interface to the next hop.

Restrictions and guidelines

This feature does not allocate End.DX4 or End.DX6 SIDs to direct routes.

Prerequisites

In the IP L3VPN over SRv6 scenario:

Before you perform this task in BGP-VPN IPv4 or IPv6 unicast address family view, execute the **segment-routing ipv6 locator** command in the same view to apply a locator to the view. This ensures successful dynamic End.DX4 or End.DX6 SID allocation.

In the public network IP over SRv6 scenario:

Before you perform this task in BGP IPv4 or BGP IPv6 unicast address family view, execute the **segment-routing ipv6 locator** command in the same view to apply a locator to the view. This ensures successful dynamic End.DX6 SID allocation.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP IPv4/IPv6 unicast address family view or BGP-VPN IPv4/IPv6 unicast address family view:
 - Enter BGP IPv4 unicast address family view.
address-family ipv4 [unicast]
 - Enter BGP IPv6 unicast address family view.
address-family ipv6 [unicast]
 - Execute the following commands in sequence to enter BGP-VPN IPv4 unicast address family view:
ip vpn-instance vpn-instance-name
address-family ipv4 [unicast]
 - Execute the following commands in sequence to enter BGP-VPN IPv6 unicast address family view:
ip vpn-instance vpn-instance-name
address-family ipv6 [unicast]
4. Allocate End.DX4 or End.DX6 SIDs to the next hops of BGP routes.
 - Allocate End.DX4 or End.DX6 SIDs to all next hops of BGP routes.
segment-routing ipv6 apply-sid all-nexthop
 - Execute the following commands in sequence to allocate End.DX4 or End.DX6 SIDs to the specified next hop of BGP routes.
segment-routing ipv6 apply-sid specify-nexthop
nexthop nexthop-address interface interface-type interface-number

By default, VPN instance-based SID allocation is used for private network routes, and the PE allocates the same SIDs to all BGP public network routes.

Command reference

nexthop interface (BGP-VPN IPv4 SR next hop view/BGP-VPN IPv4 EVPN SR next hop view)

Use **nexthop interface** to specify a next hop to which an End.DX4 SID can be dynamically allocated and specify the output interface of the next hop.

Use **undo nexthop** to restore the default.

Syntax

nexthop nexthop-address interface interface-type interface-number

undo nexthop nexthop-address

Default

No End.DX4 SID is allocated to a next hop.

Views

BGP-VPN IPv4 SR next hop view

BGP-VPN IPv4 EVPN SR next hop view

Predefined user roles

network-admin

Parameters

nexthop-address: Specifies a next hop by its IPv4 address.

interface-type interface-number: Specifies an output interface by its type and number.

Usage guidelines

This command is applicable to the IPv4 L3VPN over SRv6 or IPv4 EVPN L3VPN over SRv6 scenario to accelerate traffic forwarding. This command allocates an End.DX4 SID to the specified next hop for BGP IPv4 routes and associates the next hop with an output interface.

Use one of the following methods to allocate End.DX4 SIDs to next hops:

- Use this command to dynamically allocate an End.DX4 SID to a next hop from the locator applied to the VPN instance.
Make sure the output interface specified for the next hop in this command is consistent with the output interface of that next hop in the routing table. If they are inconsistent, the device cannot dynamically allocate an End.DX4 SID to the next hop.
- Use the **opcode end-dx4 vpn-instance** command to manually configure an End.DX4 SID in the locator applied to the VPN instance.
Make sure the output interface specified for the next hop in the **opcode end-dx4 vpn-instance** command is consistent with the output interface of that next hop in the routing table. If they are inconsistent, the device cannot use the manually configured End.DX4 SID to forward traffic.

If both methods are used for the same next hop, the manually configured End.DX4 SID takes precedence over the dynamically allocated one.

You can specify only one output interface for one next hop. To change the output interface of a next hop, first use the **undo nexthop** command to remove the original next hop and output interface association.

The device might be unable to dynamically allocate SIDs to BGP IPv4 routes based on the route next hops when dynamic SID resources are insufficient. If the device does not have manually configured End.DX4 SIDs, it allocates the End.DT4 SID or End.DT46 SID of the VPN instance to the routes.

Examples

In BGP-VPN IPv4 SR next hop view, allow the system to allocate an End.DX4 SID to next hop 10.1.1.2 and specify GigabitEthernet 1/0/1 as the output interface of the next hop.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpna
[Sysname-bgp-default-vpna] address-family ipv4 unicast
[Sysname-bgp-default-ipv4-vpna] segment-routing ipv6 locator aaa
[Sysname-bgp-default-ipv4-vpna] segment-routing ipv6 apply-sid specify-nexthop
[Sysname-bgp-default-sid-np-ipv4-vpna] nexthop 10.1.1.2 interface gigabitethernet 1/0/1
```

Related commands

opcode

nexthop interface (BGP SRv6 next hop view/BGP-VPN SRv6 next hop view/BGP-VPN IPv6 EVPN SR next hop view)

Use **nexthop interface** to specify a next hop to which an End.DX6 SID can be dynamically allocated and specify the output interface of the next hop.

Use **undo nexthop** to restore the default.

Syntax

nexthop *nexthop-ipv6-address* **interface** *interface-type interface-number*

undo nexthop *nexthop-ipv6-address*

Default

No End.DX6 SID is allocated to a next hop.

Views

BGP-VPN SRv6 next hop view

BGP-VPN IPv6 EVPN SR next hop view

BGP SRv6 next hop view

Predefined user roles

network-admin

Parameters

nexthop-ipv6-address: Specifies a next hop by its IPv6 address.

interface-type interface-number: Specifies an output interface by its type and number.

Usage guidelines

This command is applicable to the IPv6 L3VPN over SRv6, IPv6 EVPN L3VPN over SRv6, or public network IPv6 over SRv6 scenario to accelerate traffic forwarding. This command allocates an End.DX6 SID to the specified next hop for BGP IPv6 routes and associates the next hop with an output interface.

Use one of the following methods to allocate End.DX6 SIDs to next hops:

- Use this command to dynamically allocate an End.DX6 SID to a next hop from the locator applied to the VPN instance or public instance.
Make sure the output interface specified for the next hop in this command is consistent with the output interface of that next hop in the routing table. If they are inconsistent, the device cannot dynamically allocate an End.DX6 SID to the next hop.
- Use the **opcode end-dx6 vpn-instance** command to manually configure an End.DX6 SID in the locator applied to the VPN instance or public instance.
Make sure the output interface specified for the next hop in the **opcode end-dx6 vpn-instance** command is consistent with the output interface of that next hop in the routing table. If they are inconsistent, the device cannot use the manually configured End.DX6 SID to forward traffic.

If both methods are used for the same next hop, the manually configured End.DX6 SID takes precedence over the dynamically allocated one.

You can specify only one output interface for one next hop. To change the output interface of a next hop, first use the **undo nexthop** command to remove the original next hop and output interface association.

The device might be unable to dynamically allocate SIDs to BGP IPv6 routes based on the route next hops when dynamic SID resources are insufficient. If the device does not have manually configured End.DX6 SIDs, it allocates the End.DT6 SID or End.DT46 SID of the VPN instance or public instance to the routes.

Examples

In BGP SRv6 next hop view, allow the system to allocate an End.DX6 SID to next hop 10::1:2 and specify GigabitEthernet 1/0/1 as the output interface of the next hop.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv6 unicast
[Sysname-bgp-default-ipv6] segment-routing ipv6 locator aaa
[Sysname-bgp-default-ipv6] segment-routing ipv6 apply-sid specify-nexthop
[Sysname-bgp-default-sid-np-ipv6] nexthop 10::1:2 interface gigabitethernet 1/0/1
```

Related commands

opcode

segment-routing ipv6 apply-sid all-nexthop (BGP IPv4/BGP IPv6 address family view)

Use **segment-routing ipv6 apply-sid all-nexthop** to dynamically allocate an End.DX4 or End.DX6 SID to each next hop of BGP IPv6 routes in the public network.

Use **undo segment-routing ipv6 apply-sid all-nexthop** to restore the default.

Syntax

segment-routing ipv6 apply-sid all-nexthop

undo segment-routing ipv6 apply-sid all-nexthop

Default

A PE allocates the End.DT4, End.DT6, or End.DT46 SID of the public instance to BGP IPv4 or IPv6 routes in the public network.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

Use this command to forward an SRv6 decapsulated public network packet to the next hop without looking up the routing table of the public network.

This command is applicable to the public network IPv6 over SRv6 scenarios. By default, a PE allocates the same SID to all BGP public network routes. When the PE removes the SRv6 encapsulation from a received packet, it looks up the routing table of the public network based on the SID for an optimal route. To forward the packet to the next hop without looking up the routing table, use this command.

This command dynamically allocates an End.DX4 or End.DX6 SID to each next hop for BGP IPv6 routes in the public network. When forwarding a packet, the PE searches for the output interface and next hop based on the End.DX4 or End.DX6 SID of the packet. Then, the PE directly forwards the packet out of the output interface to the next hop.

Before you use this command in BGP IPv6 unicast address family view, execute the **segment-routing ipv6 locator** command in the same view to apply a locator to the view. This ensures successful dynamic End.DX4 or End.DX6 SID allocation.

In the same view, the **segment-routing ipv6 apply-sid all-nexthop** command is mutually exclusive with the **segment-routing ipv6 apply-sid specify-nexthop** command. Do not use both commands in the same view.

The device might be unable to dynamically allocate SIDs to BGP public network routes based on the route next hops when dynamic SID resources are insufficient. If the device does not have manually configured End.DX4 or End.DX6 SIDs, it allocates the End.DT4 SID, End.DT6 SID, or End.DT46 SID of the public instance to the routes.

The **segment-routing ipv6 apply-sid all-nexthop** command does not assign End.DX6 SIDs to direct routes.

Examples

In BGP IPv6 unicast address family view, enable the system to automatically allocate an End.DX6 SID to each next hop of BGP public network routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv6 unicast
[Sysname-bgp-default-ipv6] segment-routing ipv6 locator aaa
[Sysname-bgp-default-ipv6] segment-routing ipv6 apply-sid all-nexthop
```

Related commands

segment-routing ipv6 apply-sid specify-nexthop

segment-routing ipv6 locator

segment-routing ipv6 apply-sid specify-nexthop (BGP IPv4/BGP IPv6 address family view)

Use **segment-routing ipv6 apply-sid specify-nexthop** to configure next hop-specific dynamic End.DX4 or End.DX6 SID allocation for BGP public network IPv4 or IPv6 routes, and create and enter BGP SRv6 next hop view. If the view already exists, the command directly places you in the view.

Use **undo segment-routing ipv6 apply-sid specify-nexthop** to restore the default.

Syntax

segment-routing ipv6 apply-sid specify-nexthop

undo segment-routing ipv6 apply-sid specify-nexthop

Default

A PE allocates the End.DT4 SID, End.DT6 SID, or End.DT46 SID of the public instance to BGP public network IPv4 or IPv6 routes.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

This command is applicable to the public network IPv4 over SRv6 and IPv6 over SRv6 scenarios.

By default, a PE allocates the same SID to all BGP public network routes. When a PE removes the SRv6 encapsulation from a received packet, it looks up the routing table of the public network based on the SID for an optimal route. To forward the packet to the next hop without looking up the routing table, use this command and the **nexthop interface** command.

This command and the **nexthop interface** command dynamically allocate an End.DX4 or End.DX6 SID to the specified next hop. When forwarding a packet, the PE searches for the output interface and next hop based on the End.DX4 or End.DX6 SID of the packet. Then, the PE directly forwards the packet out of the output interface to the next hop.

Before you use the **segment-routing ipv6 apply-sid specify-nexthop** command in BGP IPv6 unicast address family view, execute the **segment-routing ipv6 locator** command in the same view to apply a locator to the view. This ensures successful dynamic End.DX4 or End.DX6 SID allocation.

In the same view, the **segment-routing ipv6 apply-sid specify-nexthop** command is mutually exclusive with the **segment-routing ipv6 apply-sid all-nexthop** command. Do not use both commands in the same view.

The device might be unable to dynamically allocate SIDs to BGP public network routes based on the route next hops when dynamic SID resources are insufficient. If the device does not have manually configured End.DX4 or End.DX6 SIDs, it allocates the End.DT4 SID, End.DT6 SID, or End.DT46 SID of the public instance to the routes.

The **segment-routing ipv6 apply-sid specify-nexthop** command does not assign End.DX4 or End.DX6 SIDs to direct routes.

Examples

In BGP IPv6 unicast address family view, configure next hop-specific dynamic End.DX6 SID allocation for BGP public network IPv6 routes, and create and enter BGP SRv6 next hop view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv6 unicast
[Sysname-bgp-default-ipv6] segment-routing ipv6 locator aaa
[Sysname-bgp-default-ipv6] segment-routing ipv6 apply-sid specify-nexthop
[Sysname-bgp-default-sid-np-ipv6]
```

Related commands

nexthop interface

segment-routing ipv6 apply-sid all-nexthop

segment-routing ipv6 locator

segment-routing ipv6 apply-sid specify-nexthop (BGP-VPN IPv4/IPv6 address family view)

Use **segment-routing ipv6 apply-sid specify-nexthop** to configure next hop-specific dynamic End.DX4 or End.DX6 SID allocation for BGP private network IPv4 or IPv6 routes, and create and enter BGP-VPN IPv4 SR or SRv6 next hop view. If the view already exists, the command directly places you in the view.

Use **undo segment-routing ipv6 apply-sid specify-nexthop** to restore the default.

Syntax

```
segment-routing ipv6 apply-sid specify-nexthop [ evpn ]  
undo segment-routing ipv6 apply-sid specify-nexthop [ evpn ]
```

Default

A PE allocates the End.DT4, End.DT6, or End.DT46 SID of a VPN instance to the BGP private network IPv4 or IPv6 routes of that VPN instance.

Views

BGP-VPN IPv4 unicast address family view
BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

evpn: Enables next hop-specific dynamic End.DX4 or End.DX6 SID allocation for private network routes when the routes are converted to BGP EVPN routes in an EVPN L3VPN over SRv6 network. If you do not specify this keyword, this command enables nexthop-specific dynamic End.DX4 or End.DX6 SID allocation for private network routes when the routes are converted to BGP VPNv4 or VPNv6 routes.

Usage guidelines

This command is applicable to the MPLS L3VPN over SRv6 and EVPN L3VPN over SRv6 scenarios.

By default, a PE allocates the same SID to all BGP routes of a VPN instance. When the PE removes the SRv6 encapsulation from a received packet, it looks up the routing table of the VPN instance based on the SID for an optimal route. Then, the PE forwards the packet to a CE. To forward the packet to the next hop without looking up the routing table, use this command and the **nexthop interface** command.

This command and the **nexthop interface** command dynamically allocate an End.DX4 or End.DX6 SID to the specified next hop. When forwarding a packet, the PE searches for the output interface and next hop based on the End.DX4 or End.DX6 SID of the packet. Then, the PE directly forwards the packet out of the output interface to the next hop.

Before you use the **segment-routing ipv6 apply-sid specify-nexthop** command in BGP-VPN IPv4 or IPv6 unicast address family view, execute the **segment-routing ipv6 locator** command in the same view to apply a locator to the view. This ensures successful dynamic End.DX4 or End.DX6 SID allocation.

In the same view, the **segment-routing ipv6 apply-sid specify-nexthop** command is mutually exclusive with the **segment-routing ipv6 apply-sid all-nexthop** command. Do not use both commands in the same view.

The device might be unable to dynamically allocate SIDs to BGP private network routes in a VPN instance based on the route next hops when dynamic SID resources are insufficient. If the device does not have manually configured End.DX4 or End.DX6 SIDs, it allocates the End.DT4 SID, End.DT6 SID, or End.DT46 SID of the VPN instance to the routes.

Examples

In BGP-VPN IPv4 unicast address family view, configure next hop-specific dynamic End.DX4 SID allocation for BGP private network IPv4 routes, and create and enter BGP-VPN IPv4 SR next hop view.

```
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp-default] ip vpn-instance vpn1
```

```
[Sysname-bgp-default-vpn1] address-family ipv4 unicast
[Sysname-bgp-default-ipv4-vpn1] segment-routing ipv6 locator aaa
[Sysname-bgp-default-ipv4-vpn1] segment-routing ipv6 apply-sid specify-nexthop
[Sysname-bgp-default-sid-np-ipv4]
```

Related commands

nexthop interface

segment-routing ipv6 apply-sid all-nexthop

segment-routing ipv6 locator

New feature: VPNv4/VPNv6/EVPN routes

Modifying BGP VPNv4 or VPNv6 routes

About this task

Configure this feature on an MPE that connects the MPLS L3VPN and L3VPN over SRv6 networks. This feature enables the MPE to modify BGP VPNv4 or VPNv6 route information for intercommunication between the MPLS and SRv6 networks.

After you configure this feature on an MPE, the MPE performs the following operations after receiving BGP VPNv4 or VPNv6 routes from the MPLS L3VPN network:

1. Matches the route targets of the routes with the import route targets of local VPN instances.
2. Replaces the RD and route targets of the routes with those of the matching local VPN instance. In addition, the MPE adds an SRv6 SID to the routes and maps the SRv6 SID of the routes to the private label of the routes.
3. Advertises the reoriginated routes to the SRv6 network.

After you configure this feature on an MPE, the MPE performs the following operations after receiving BGP VPNv4 or VPNv6 routes from the SRv6 network:

1. Matches the route targets of the routes with the import route targets of local VPN instances.
2. Replaces the RD and route targets of the routes with those of the matching local VPN instance. In addition, the MPE adds an MPLS label to the routes and maps the private label of the routes to the SRv6 SID of the routes.
3. Advertises the reoriginated routes to the MPLS L3VPN network.

Restrictions and guidelines

All settings in this section are configured on an MPE.

In addition to the settings in this section, you also need to configure other settings on the UPEs, MPE, and SPE depending on the network type. If the network type is MPLS, configure basic MPLS L3VPN settings. If the network type is SRv6, configure basic IP L3VPN over SRv6 settings.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP VPNv4, VPNv6, or EVPN address family view.
 - o Enter BGP VPNv4 address family view.
address-family vpnv4

- Enter BGP VPNv6 address family view.
address-family vpnv6
- Enter BGP EVPN address family view.
address-family l2vpn evpn
- 4. Enable the device to reoriginate BGP EVPN, VPNv4 or VPNv6 routes based on the BGP EVPN, VPNv4 or VPNv6 routes received from a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
re-originated [**replace-rt**]
By default, the device does not reoriginate BGP EVPN, VPNv4 or VPNv6 routes based on received BGP VPNv4 or VPNv6 routes.
- 5. (Optional.) Enable the device to advertise original BGP EVPN, VPNv4 or VPNv6 routes to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
advertise original-route
By default, the device advertises only reoriginated BGP EVPN, VPNv4 or VPNv6 routes to peers and peer groups after the **peer re-originated** command is executed.
- 6. (Optional.) Suppress advertisement of reoriginated BGP EVPN, VPNv4 or VPNv6 routes to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
suppress re-originated
By default, the device advertises reoriginated BGP EVPN, VPNv4 or VPNv6 routes to peers and peer groups after the **peer re-originated** command is executed.

Command reference

peer re-originated

Use **peer re-originated** to enable the device to reoriginate BGP VPNv4, VPNv6, or EVPN routes based on the BGP VPNv4, VPNv6, or EVPN routes received from a peer or peer group.

Use **undo peer re-originated** to disable the device from reoriginating BGP VPNv4, VPNv6, or EVPN routes based on the BGP VPNv4, VPNv6, or EVPN routes received from a peer or peer group.

Syntax

In BGP VPNv4 address family view or BGP VPNv6 address family view:

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
re-originated [ replace-rt ]
```

```
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
re-originated
```

In BGP EVPN address family view:

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
re-originated [ ip-prefix ] [ replace-rt ]
```

```
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
re-originated [ ip-prefix ]
```


Default

The device does not reoriginate BGP VPNv4, VPNv6, or EVPN routes based on received BGP VPNv4, VPNv6, or EVPN routes.

Views

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must exist.

ipv4-address: Specifies a peer by its IPv4 address. The peer must exist.

mask-length: Specifies a mask length in the range of 0 to 32. To specify a subnet, you must specify both the *ipv4-address* and *mask-length* arguments.

ipv6-address: Specifies a peer by its IPv6 address. The peer must exist.

prefix-length: Specifies a prefix length in the range of 0 to 128. To specify a subnet, you must specify both the *ipv6-address* and *prefix-length* arguments.

ip-prefix: Specifies IP prefix advertisement routes. If you do not specify this keyword, the command still reoriginates IP prefix advertisement routes.

replace-rt: Modifies route information.

- Replaces the RD and route targets of VPNv4 or VPNv6 routes with those of the matching local VPN instance, and adds MPLS labels or SRv6 SIDs to the routes. If you do not specify this keyword, the device performs the same operations except that it does not replace the route targets.
- Replaces the L3 VXLAN ID, RD, and route targets of EVPN IP prefix advertisement routes with those of the matching local VPN instance, and adds MPLS labels or SRv6 SIDs to the routes. If you do not specify this keyword, the device performs the same operations except that it does not replace the route targets.

Usage guidelines

Use this command on a PE that connects the MPLS L3VPN and MPLS L3VPN over SRv6 networks or connects the EVPN L3VPN and EVPN L3VPN over SRv6 networks. This command enables the PE to modify VPNv4, VPNv6, or EVPN route information to realize intercommunication between the MPLS and SRv6 networks.

After you execute this command on a PE, the PE performs the following operations after receiving BGP VPNv4, VPNv6, or EVPN routes from the MPLS L3VPN or EVPN L3VPN network:

1. Matches the route targets of the routes with the import route targets of local VPN instances.
2. Replaces the L3 VXLAN ID (for EVPN L3VPN), RD, and route targets of the routes with those of the matching local VPN instance. In addition, the PE adds an SRv6 SID to the routes and maps the SRv6 SID of the routes to the private label of the routes.
3. Advertises the reoriginated routes to the SRv6 network.

After you execute this command on a PE, the PE performs the following operations after receiving BGP VPNv4, VPNv6, or EVPN routes from the SRv6 network:

4. Matches the route targets of the routes with the import route targets of local VPN instances.
5. Replaces the L3 VXLAN ID (for EVPN L3VPN), RD, and route targets of the routes with those of the matching local VPN instance. In addition, the PE adds MPLS labels to the routes and maps the private label of the routes to the SRv6 SID of the routes.

6. Advertises the reoriginated routes to the MPLS L3VPN or EVPN L3VPN network.

After you execute this command on a PE, the PE advertises only reoriginated routes to the specified peer or peer group. The original routes are not advertised.

If the RD of a received BGP VPNv4, VPNv6, or EVPN route is identical to the RD of the matching local VPN instance, a PE does not modify the route or reoriginate the route. As a result, the PE does not advertise the route. As a best practice, assign unique RDs to VPN instances on different devices if you use this command.

Examples

In BGP VPNv4 address family view, replace the RD and route targets of the BGP VPNv4 routes received from peer 1.1.1.1 and add an MPLS label or SRv6 SID to the routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family vpnv4
[Sysname-bgp-default-vpnv4] peer 1.1.1.1 re-originated replace-rt
```

Related commands

peer advertise original-route

peer suppress re-originated

peer suppress re-originated

Use **peer suppress re-originated** to suppress advertisement of reoriginated BGP VPNv4, VPNv6, or EVPN routes to a peer or peer group.

Use **undo peer suppress re-originated** to restore the default.

Syntax

In BGP VPNv4 address family view or BGP VPNv6 address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
suppress re-originated

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
suppress re-originated

In BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
suppress re-originated ip-prefix

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
suppress re-originated ip-prefix

Default

The device advertises reoriginated BGP VPNv4, VPNv6, or EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

Views

BGP VPNv4 address family view

BGP VPNv6 address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must exist.

ipv4-address: Specifies a peer by its IPv4 address. The peer must exist.

mask-length: Specifies a mask length in the range of 0 to 32. To specify a subnet, you must specify both the *ipv4-address* and *mask-length* arguments.

ipv6-address: Specifies a peer by its IPv6 address. The peer must exist.

prefix-length: Specifies a prefix length in the range of 0 to 128. To specify a subnet, you must specify both the *ipv6-address* and *prefix-length* arguments.

ip-prefix: Specifies IP prefix advertisement routes.

Usage guidelines

The device configured with the **peer re-originated** and **peer advertise original-route** commands advertises both original and reoriginated BGP VPNv4, VPNv6, or EVPN routes. For the device to advertise only original BGP VPNv4, VPNv6, EVPN routes to a peer or peer group, execute the **peer suppress re-originated** command on the device.

Examples

In BGP VPNv4 address family view, suppress advertisement of reoriginated BGP VPNv4 routes to peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family vpnv4
[Sysname-bgp-default-vpnv4] peer 1.1.1.1 suppress re-originated
```

Related commands

peer advertise original-route

peer re-originated

New feature: G-SRv6

Configuring G-SIDs

About this task

In an SRv6 TE policy scenario, the administrator needs to add the 128-bit SRv6 SIDs of SRv6 nodes on the packet forwarding path into the SID list of the SRv6 TE policy. If the packet forwarding path is long, a large number of SRv6 SIDs will be added to the SID list of the SRv6 TE policy. This greatly increases the size of the SRv6 packet header, resulting in low device forwarding efficiency and reduced chip processing speed. The situation might be worse in a scenario that spans across multiple ASs where a much greater number of end-to-end SRv6 SIDs exist.

Generalized SRv6 (G-SRv6) encapsulates shorter SRv6 SIDs (G-SIDs) in the segment list of SRH by compressing the 128-bit SRv6 SIDs. This reduces the size of the SRv6 packet header and improves the efficiency for forwarding SRv6 packets. In addition, G-SRv6 supports both 128-bit SRv6 SIDs and G-SIDs in a segment list.

Typically, an address space is reserved for SRv6 SID allocation in an SRv6 subnet. This address space is called an SID space. In the SRv6 subnet, all SIDs are allocated from the SID space. The SIDs have the same prefix (common prefix). The SID common prefix is redundant information in the SRH.

G-SRv6 removes the common prefix and carries only the variable portion of SRv6 SIDs (G-SIDs) in the segment list, effectively reducing the SRv6 packet header size. To forward a packet according to routing table lookup, SRv6 replaces the destination IP address of the packet with the combination of the G-SID and common prefix in the segment list of the SRH.

With the compression efficiency and network scale taken into consideration, the ideal length of SRv6 SIDs is 32 bits after compression through G-SRv6.

Restrictions and guidelines

The IPv6 prefix length must be longer than the common prefix length.

Configuring an opcode

1. Enter system view.
system-view
2. Enable SRv6 and enter SRv6 view.
segment-routing ipv6
3. Enable SRv6 compression.
srv6 compress enable
By default, SRv6 compression is disabled.
4. Configure a locator and enter SRv6 locator view.
locator locator-name [ipv6-prefix ipv6-address prefix-length common-prefix common-prefix-length coc32 [args args-length | static static-length] *]
5. Configure an opcode. Perform one of the following tasks:
 - Configure an End SID.
opcode opcode end-coc32 [no-psp]
 - Configure an End.X SID.
opcode opcode end-x-coc32 interface interface-type interface-number nexthop nexthop-address [no-psp]

Using IS-IS to advertise SRv6 SIDs

1. Enter system view.
system-view
2. Enter IS-IS process view.
isis [process-id] [vpn-instance vpn-instance-name]
3. Enter IS-IS IPv6 address family view.
address-family ipv6 [unicast]
4. Apply a locator to IS-IS IPv6 address family.
segment-routing ipv6 locator locator-name [level-1 | level-2] [auto-sid-disable]
By default, no locators are applied to IS-IS IPv6 address family.
Repeat this command to apply multiple locators to IS-IS IPv6 address family for the family to advertise multiple SRv6 SIDs.
5. Enable SRv6 compression for IPv6 IS-IS.
srv6 compress enable [level-1 | level-2]
By default, SRv6 compression is disabled for IPv6 IS-IS.
Use this command only when IPv6 IS-IS is used to advertise G-SIDs.

Command reference

New command: `srv6 compress enable` (IS-IS IPv6 address family view)

Use **`srv6 compress enable`** to enable SRv6 compression for IPv6 IS-IS.

Use **`undo srv6 compress enable`** to disable SRv6 compression for IPv6 IS-IS.

Syntax

`srv6 compress enable [ level-1 | level-2 ]`

`undo srv6 compress enable`

Default

SRv6 compression is disabled for IPv6 IS-IS.

Views

IS-IS IPv6 address family view

Predefined user roles

network-admin

Parameters

level-1: Specifies the level-1 area.

level-2: Specifies the level-2 area.

Usage guidelines

If you do not specify a level, this command enables SRv6 compression for both level-1 and level-2 areas.

If IPv6 IS-IS is used to advertise G-SIDs to neighbors, you must use this command to enable SRv6 compression for IPv6 IS-IS.

Use this command only when the cost style of IS-IS is **wide**, **compatible**, or **wide-compatible**.

Before you use this command, apply a locator to IS-IS IPv6 address family view by using the **`segment-routing ipv6 locator`** command.

Examples

Enable SRv6 compression for IPv6 IS-IS.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] cost-style wide
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] srv6 compress enable
```

Related commands

`segment-routing ipv6 locator` (IS-IS IPv6 address family)

New command: `srv6 compress enable` (Segment Routing IPv6 view)

Use **`srv6 compress enable`** to enable SRv6 compression.

Use **undo srv6 compress enable** to disable SRv6 compression.

Syntax

srv6 compress enable

undo srv6 compress enable

Default

SRv6 compression is disabled.

Views

SRv6 view

Predefined user roles

network-admin

Usage guidelines

Typically, an address space is reserved for SRv6 SID allocation in an SRv6 subnet. This address space is called an SID space. In the SRv6 subnet, all SIDs are allocated from the SID space. The SIDs have the same prefix (common prefix). The SID common prefix is redundant information in the SRH.

SRv6 compression removes the common prefix from the SIDs in the SID list of the SRH. The remaining part of an SID is called a G-SID. G-SIDs reduce the cost of SRH.

When SRv6 uses the SID list in the SRH to replace the destination address of a packet, it combines the common prefix and the destination G-SID to form a new SID. This new SID is used as the destination address of the packet.

Examples

Enable SRv6 compression.

```
<Sysname> system-view
```

```
[Sysname] segment-routing ipv6
```

```
[Sysname-segment-routing-ipv6] srv6 compress enable
```

Modified command: locator

Use **locator** to create an SRv6 locator and enter its view, or enter the view of an existing SRv6 locator.

Use **undo locator** to delete an SRv6 locator.

Old syntax

locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]

undo locator *locator-name*

New syntax

locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]

locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* **common-prefix** *common-prefix-length* **coc32** [**args** *args-length* | **static** *static-length*] *]

undo locator *locator-name*

Views

SRv6 view

Change description

The following parameters are added:

common-prefix *common-prefix-length*: Specifies the G-SID common prefix length. The value range for the *common-prefix-length* argument varies by the value of the *prefix-length* argument and varies by device model. If you do not specify a G-SID common prefix length, the common prefix length is 0.

coc32: Enables 32-bit G-SID compression.

Modified command: opcode

Use **opcode** to configure the opcode of an SRv6 SID.

Use **undo opcode** to delete the opcode of an SRv6 SID.

Old syntax

```
opcode opcode end [ no-psp ]
```

```
opcode opcode end-x interface interface-type interface-number nexthop  
nexthop-ipv6-address [ no-psp ]
```

```
opcode opcode end-dt4 [ vpn-instance vpn-instance-name [ evpn ] ]
```

```
opcode opcode end-dt46 [ vpn-instance vpn-instance-name [ evpn ] ]
```

```
opcode opcode end-dt6 [ vpn-instance vpn-instance-name [ evpn ] ]
```

```
opcode opcode end-dx4 interface interface-type interface-number nexthop  
nexthop-ipv4-address [ vpn-instance vpn-instance-name [ evpn ] ]
```

```
opcode opcode end-dx6 interface interface-type interface-number nexthop  
nexthop-ipv6-address [ vpn-instance vpn-instance-name [ evpn ] ]
```

```
opcode opcode end-op
```

New syntax

```
opcode { opcode | hex hex-opcode } end [ no-psp ]
```

```
opcode { opcode | hex hex-opcode } end-x interface interface-type interface-number  
nexthop nexthop-ipv6-address [ no-psp ]
```

```
opcode { opcode | hex hex-opcode } end-coc32 [ no-psp ]
```

```
opcode { opcode | hex hex-opcode } end-x-coc32 interface interface-type interface-number  
nexthop nexthop-ipv6-address [ no-psp ]
```

```
opcode { opcode | hex hex-opcode } end-dt4 [ vpn-instance vpn-instance-name [ evpn |  
l3vpn-evpn ] ]
```

```
opcode { opcode | hex hex-opcode } end-dt46 [ vpn-instance vpn-instance-name [ evpn |  
l3vpn-evpn ] ]
```

```
opcode { opcode | hex hex-opcode } end-dt6 [ vpn-instance vpn-instance-name [ evpn |  
l3vpn-evpn ] ]
```

```
opcode { opcode | hex hex-opcode } end-dx4 interface interface-type interface-number  
nexthop nexthop-ipv4-address [ vpn-instance vpn-instance-name [ evpn ] ]
```

```
opcode { opcode | hex hex-opcode } end-dx6 interface interface-type interface-number  
nexthop nexthop-ipv6-address [ vpn-instance vpn-instance-name [ evpn ] ]
```

```

opcode { opcode | hex hex-opcode } end-dx2 xconnect-group group-name connection
connection-name

opcode { opcode | hex hex-opcode } end-dx2 vsi vsi-name interface interface-type
interface-number

opcode { opcode | hex hex-opcode } end-dx2l xconnect-group group-name connection
connection-name

opcode { opcode | hex hex-opcode } end-dx2l vsi vsi-name interface interface-type
interface-number

opcode { opcode | hex hex-opcode } end-dt2m vsi vsi-name

opcode { opcode | hex hex-opcode } end-dt2u vsi vsi-name

opcode { opcode | hex hex-opcode } end-dt2ul vsi vsi-name

opcode { opcode | hex hex-opcode } end-op

opcode { opcode | hex hex-opcode } end-m mirror-locator ipv6-address prefix-length

undo opcode { opcode | hex hex-opcode } [ end-m mirror-locator ipv6-address
prefix-length ]

```

Views

SRv6 locator view

Change description

The following parameters are added:

end-coc32: Specifies the End (COC32) type.

end-x-coc32: Specifies the End.X (COC32) type.

end-dx2l: Specifies the End.DX2L type.

end-dt2m: Specifies the End.DT2M type.

end-dt2u: Specifies the End.DT2U type.

end-dt2ul: Specifies the End.DT2UL type.

end-m: Specifies the End.M type.

l3vpn-evpn: Specifies EVPN routes, VPNv4 routes, and VPNv6 routes.

xconnect-group *group-name*: Specifies the cross-connect group to which the SRv6 SID belongs. The *group-name* argument represents the cross-connect group name, a case-sensitive string of 1 to 31 characters. The name cannot contain a hyphen (-). The specified cross-connect group must exist.

connection *connection-name*: Specifies the cross-connect to which the SRv6 SID belongs. The *connection-name* argument represents the cross-connect name, a case-sensitive string of 1 to 20 characters. The name cannot contain a hyphen (-). The specified cross-connect must exist.

vsi *vsi-name*: Specifies the VSI to which the SRv6 SID belongs. The *vsi-name* argument represents the VSI name, a case-sensitive string of 1 to 31 characters. The specified VSI must exist.

mirror-locator *ipv6-address* *prefix-length*: Specifies a protected locator by its IPv6 address prefix and prefix length. The *ipv6-address* argument represents the IPv6 address prefix. The *prefix-length* argument represents the prefix length, in the range of 32 to 120. Make sure the specified locator is the same as the locator on a protected node.

New feature: Configuring the SRv6 MTU

Configuring the SRv6 MTU

About this task

Perform this task to configure one of the following MTUs:

- **Path MTU**—The maximum IPv6 MTU along the path from the source node to the destination node. The transit nodes do not fragment SRv6 tunneled packets. If a packet is larger than the MTU of the output interface, the packet will be discarded. If the MTU is too small, the bandwidth is not sufficiently used. To address these issues, configure an appropriate SRv6 path MTU.
- **Reserved MTU**—Reserved MTU on the source node for TI-LFA. When packets are switched to the backup path after the primary path fails, the device reconstructs an IPv6 header and SRH for the packets. As a result, packet drop might occur because the packet size has exceeded the MTU. To resolve this issue, configure a reserved MTU on the source node to reserve bytes for adding a new SRH to SRv6 packets in case of primary path failure.

The SRv6 path MTU minus the reserved MTU is the active MTU. The effective MTU for SRv6 packets on the source node is the smaller value from the following values:

- The active MTU.
- The IPv6 MTU of the physical output interface.

Restrictions and guidelines

Make sure the active MTU is equal to or greater than 1280 bytes.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Specify a reserved MTU for SRv6 path MTU.
path-mtu reserved [*reserved-value*]
By default, no reserved MTU is specified for SRv6 path MTU.
4. Configure the SRv6 path MTU.
path-mtu *mtu-value*
By default, the SRv6 path MTU is 1500 bytes.

Command reference

New command: path-mtu reserved

Use **path-mtu reserved** to specify a reserved MTU for SRv6 path MTU.

Use **undo path-mtu reserved** to restore the default.

Syntax

path-mtu reserved [*reserved-value*]

undo path-mtu reserved

Default

No reserved MTU is specified for SRv6 path MTU.

Views

SRv6 view

Predefined user roles

network-admin

Parameters

reserved-value: Specifies an MTU value, in bytes. The default value is 72 bytes.

Usage guidelines

Use this command in the TI-LFA scenario. When packets are switched to the backup path after the primary path fails, the device reconstructs an IPv6 header and SRH for the packets. As a result, packet drop might occur because the packet size has exceeded the MTU. To resolve this issue, configure a reserved MTU on the source node to reserve bytes for adding a new SRH to SRv6 packets in case of primary path failure.

The SRv6 path MTU minus the reserved MTU is the active MTU. Make sure the active MTU is equal to or greater than 1280 bytes.

The effective MTU for SRv6 packets on the source node is the smaller value from the following values:

- The active MTU.
- The IPv6 MTU of the physical output interface.

For example, if the SRv6 path MTU is 1600 bytes and the reserved MTU is 100 bytes, the active MTU is 1500 bytes.

- If the IPv6 MTU of the physical output interface is equal to or greater than 1500 bytes, the effective MTU on the source node is 1500 bytes.
- If the IPv6 MTU of the physical output interface is smaller than 1500 bytes, the effective MTU on the source node is the IPv6 MTU of the physical output interface.

Examples

```
# Reserve 200 bytes for SRv6 path MTU.
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] path-mtu reserved 200
```

New feature: Configuring the SRv6 DiffServ mode

Configuring the SRv6 DiffServ mode

About this task

SRv6 DiffServ mode determines how an SRv6 node processes the IP precedence and DSCP for packets forwarded between an IP network and an SRv6 network. The device supports the following SRv6 DiffServ modes:

- **Pipe mode**—When a packet enters the SRv6 network, the ingress node adds a new IPv6 header to the original packet. The ingress node ignores the IP precedence or DSCP value in the original packet and uses the value specified by using the *service-class* argument as the traffic class in the new IPv6 header.

In the SRv6 network, SRv6 nodes perform QoS scheduling for the packet based on the specified traffic class. When the packet leaves the SRv6 network, the egress node removes the outer IPv6 header from the packet without modifying the IP precedence or DSCP value in the original packet.

- **Short-pipe mode**—When a packet enters and leaves the SRv6 network, all SRv6 nodes process the packet in the same way as in pipe mode except for the egress node. After the egress node removes the outer IPv6 header from the packet, it performs QoS scheduling as follows:
 - If no priority trust mode is configured, the egress node performs QoS scheduling for the packet based on the IP precedence or DSCP value in the original packet.
 - If a priority trust mode is configured, the egress node performs QoS scheduling for the packet based on the trusted priority.
- **Uniform mode**—When a packet enters the IPv6 network, the ingress node maps the IP precedence or DSCP value in the original IP header to the outer IPv6 header as the traffic class. When the packet leaves the SRv6 network, the egress node maps the traffic class value in the outer IPv6 header to the original packet as the IP precedence or DSCP value.

Restrictions and guidelines

When you configure the SRv6 DiffServ mode on the source and destination nodes of an SRv6 tunnel, follow these restrictions and guidelines:

- The outbound DiffServ mode on the local end must be the same as the inbound DiffServ mode on the peer end.
- The inbound DiffServ mode on the local end must be the same as the outbound DiffServ mode on the peer end.

For more information about IP precedence and DSCP, see priority mapping configuration in *QoS Configuration Guide*.

Procedure

1. Enter system view.

system-view

2. Enter SRv6 view.

segment-routing ipv6

3. Configure the SRv6 DiffServ mode.

```
diffserv-mode { ingress { pipe service-class | short-pipe service-class | uniform } egress { pipe | short-pipe | uniform } | { pipe service-class | short-pipe service-class | uniform } }
```

By default, the SRv6 DiffServ mode is pipe and uses 0 as the Traffic Class value in the new IPv6 header.

Command reference

New command: diffserv-mode

Use **diffserv-mode** to configure the SRv6 DiffServ mode.

Use **undo diffserv-mode** to restore the default.

Syntax

```
diffserv-mode { ingress { pipe service-class | short-pipe service-class | uniform } egress { pipe | short-pipe | uniform } | { pipe service-class | short-pipe service-class | uniform } }
```

undo diffserv-mode

Default

The SRv6 DiffServ mode is pipe and the traffic class value in the new IPv6 packet header is 0.

Views

SRv6 view

Predefined user roles

network-admin

Parameters

ingress: Specifies the inbound direction.

egress: Specifies the outbound direction.

pipe: Specifies the pipe mode.

short-pipe: Specifies the short-pipe mode.

uniform: Specifies the uniform mode.

service-class: Specifies a traffic class for packets that enters the SRv6 network from the IP network. The value range for the traffic class is 0 to 7.

Usage guidelines

The following SRv6 DiffServ modes are available:

- **Pipe mode**—When a packet enters the SRv6 network, the ingress node adds a new IPv6 header to the original packet. The ingress node ignores the IP precedence or DSCP value in the original packet and uses the value specified by using the *service-class* argument as the traffic class in the new IPv6 header. In the SRv6 network, SRv6 nodes perform QoS scheduling for the packet based on the specified traffic class. When the packet leaves the SRv6 network, the egress node removes the outer IPv6 header from the packet without modifying the IP precedence or DSCP value in the original packet.
- **Short-pipe mode**—When a packet enters and leaves the SRv6 network, all SRv6 nodes process the packet in the same way as in pipe mode except for the egress node. After the egress node removes the outer IPv6 header from the packet, it performs QoS scheduling as follows:
 - If no priority trust mode is configured, the egress node performs QoS scheduling for the packet based on the IP precedence or DSCP value in the original packet.
 - If a priority trust mode is configured, the egress node performs QoS scheduling for the packet based on the trusted priority.
- **Uniform mode**—When a packet enters the IPv6 network, the ingress node maps the IP precedence or DSCP value in the original IP header to the outer IPv6 header as the traffic class. When the packet leaves the SRv6 network, the egress node maps the traffic class value in the outer IPv6 header to the original packet as the IP precedence or DSCP value.

The priority accuracy has changes when the DSCP value and traffic class value are mapped to each other.

To specify different DiffServ modes for the inbound and outbound directions, use the **diffserv-mode** command with the **ingress** and **egress** keywords. To specify the same DiffServ mode for the inbound and outbound directions, use the **diffserv-mode** command without the **ingress** or **egress** keyword.

If you execute the **diffserv-mode** command multiple times, the most recent configuration takes effect.

When you configure the SRv6 DiffServ mode on the source and destination nodes of an SRv6 tunnel, follow these restrictions and guidelines:

- The outbound DiffServ mode on the local end must be the same as the inbound DiffServ mode on the peer end.

- The inbound DiffServ mode on the local end must be the same as the outbound DiffServ mode on the peer end.

For more information about IP precedence and DSCP, see priority mapping configuration in *QoS Configuration Guide*.

Examples

```
# Configure the SRv6 DiffServ mode as uniform.
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] diffserv-mode uniform
```

New feature: BGP-EPE

Configuring BGP EPE

Configuring SID allocation through BGP EPE

Restrictions and guidelines

When you configure BGP EPE, follow these restrictions and guidelines:

- By default, a BGP peering SID is node type.
- If you do not specify a SID value or a routing policy when enabling BGP EPE, the system will assign labels to BGP peers randomly.
- BGP EPE must be used together with SR-MPLS TE policy, MPLS TE, or static SRLSP. The MPLS TE tunnel requires using a static SRLSP. The outgoing label of the static SRLSP must be the same as the label specified during BGP EPE configuration.

When you use BGP EPE to apply a routing policy to a peer or peer group, follow these restrictions and guidelines:

- You cannot apply a routing policy to assign the same label to multiple BGP peers or peer groups when you assign a PeerNode SID, PeerAdj SID, or PeerNode-Adj SID to the BGP peers or peer groups.
- You can apply a routing policy to assign the same label to multiple BGP peers or peer groups only when you assign a PeerSet SID to the BGP peers or peer groups.
- You can use **if-match interface** as a filtering condition only when you assign a PeerAdj SID to a BGP peer or peer group.

Prerequisites

Before assigning BGP-EPE SIDs, execute the **display mpls label** command to display the usage status of the labels that you want to assign as BGP-EPE SIDs. Make sure the labels are in Idle state. A label that is not in Idle state is being used by another protocol. If you assign it to a peer or peer group as a BGP-EPE SID, the BGP-EPE SID is not available even if the status of the label changes to Idle later. To use the BGP-EPE SID, you must remove the BGP-EPE SID assignment and assign the BGP-EPE SID again.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enable BGP EPE and specify a routing policy for the peer or peer group.

```
peer { group-name | ipv4-address [ mask-length ] } egress-engineering [ adjacency | node-adjacency | set ] [ label label-value | route-policy policy-name ]
```

By default, BGP EPE is disabled.

4. (Optional.) Configure the label value in the routing policy.

- a. Return to system view.

```
quit
```

- b. Enter the routing policy view.

```
route-policy route-policy-name { deny | permit } node node-number
```

- c. Specify a label value.

```
apply label-value label-value
```

By default, no label value is specified.

Configuring a BGP EPE peer set

About this task

If a device has established BGP peer relationships with multiple devices, you can manually add the BGP peers to a BGP EPE peer set and assign a PeerSet SID to the set. Then, the device can send traffic to the peers in the set for load sharing when it forwards the traffic based on the PeerSet SID.

Prerequisites

Before adding a peer or peer group to a BGP EPE peer set, you must enable BGP EPE for the peer or peer group.

Before assigning BGP-EPE SIDs, execute the **display mpls label** command to display the usage status of the labels that you want to assign as BGP-EPE SIDs. Make sure the labels are in Idle state. A label that is not in Idle state is being used by another protocol. If you assign it to a peer or peer group as a BGP-EPE SID, the BGP-EPE SID is not available even if the status of the label changes to Idle later. To use the BGP-EPE SID, you must remove the BGP-EPE SID assignment and assign the BGP-EPE SID again.

Procedure

1. Enter system view.

```
system-view
```

2. Enter BGP instance view.

```
bgp as-number [ instance instance-name ]
```

3. Create a BGP EPE peer set.

```
egress-engineering peer-set peer-set-name [ label label-value ]
```

4. Add a peer or peer group to the BGP EPE peer set.

```
peer { group-name | ipv4-address [ mask-length ] } peer-set peer-set-name
```

By default, a peer or peer group does not belong to a BGP EPE peer set.

Command reference

New command: egress-engineering peer-set

Use **egress-engineering peer-set** to create a BGP EPE peer set.

Use **undo egress-engineering peer-set** to delete a BGP EPE peer set.

Syntax

```
egress-engineering peer-set peer-set-name [ label label-value ]  
undo egress-engineering peer-set peer-set-name
```

Default

No BGP EPE peer sets exist.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

peer-set-name: Specifies a BGP EPE peer set name, a case-sensitive string of 1 to 63 characters.

label *label-value*: Specifies a SID for the BGP EPE peer set. The value range for the *label-value* argument varies by device model. If you do not specify a SID, this command dynamically assigns a SID for the BGP EPE peer set.

Usage guidelines

BGP EPE assigns BGP peering SIDs to segments across ASs. The device sends BGP peering SIDs to the controller through BGP-LS extensions. The controller orchestrates IGP SIDs and BGP peering SIDs for inter-AS forwarding over optimal paths.

You can add multiple BGP peers into a BGP EPE peer set and assign a PeerSet SID to the set. A PeerSet SID corresponds to multiple outgoing interfaces.

Before assigning BGP-EPE SIDs, execute the **display mpls label** command to display the usage status of the labels that you want to assign as BGP-EPE SIDs. Make sure the labels are in Idle state. A label that is not in Idle state is being used by another protocol. If you assign it to a peer or peer group as a BGP-EPE SID, the BGP-EPE SID is not available even if the status of the label changes to Idle later. To use the BGP-EPE SID, you must remove the BGP-EPE SID assignment and assign the BGP-EPE SID again.

Examples

```
# Create a BGP EPE peer set named bgpepe, and assign SID 5555 to the set.  
<Sysname> system-view  
[Sysname] bgp 100  
[Sysname-bgp-default] egress-engineering peer-set bgpepe label 5555
```

Related commands

peer egress-engineering

peer peer-set

New command: peer peer-set

Use **peer peer-set** to add a peer or peer group to a BGP EPE peer set.

Use **undo peer peer-set** to remove a peer or peer group from its BGP EPE peer set.

Syntax

```
peer { group-name | ipv4-address [ mask-length ] } peer-set peer-set-name  
undo peer { group-name | ipv4-address [ mask-length ] } peer-set
```

Default

A peer or peer group does not belong to a BGP EPE peer set.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies an existing peer group by its name, a case-sensitive string of 1 to 47 characters.

ipv4-address: Specifies an existing peer by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. The IPv4 address and the mask length together specify a network segment. This command applies to the dynamic peers in the specified network segment.

peer-set-name: Specifies the name of the BGP EPE peer set to which the specified BGP peers will be added. The peer set name is a case-sensitive string of 1 to 63 characters.

Usage guidelines

Before you execute this command, make sure BGP EPE is enabled.

If a peer or peer group is assigned a PeerSet SID (by using the **peer egress-engineering set** command), the peer or peer group cannot be added to a BGP EPE peer set, and vice versa.

Examples

Add peer 10.1.1.1 to BGP EPE peer set **abc**.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] peer 10.1.1.1 peer-set abc
```

Related commands

egress-engineering peer-set

peer egress-engineering

New command: display bgp egress-engineering peer-set

Use **display bgp egress-engineering peer-set** to display BGP EPE peer set information.

Syntax

display bgp [**instance** *instance-name*] **egress-engineering peer-set** [*peer-set-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays BGP EPE peer set information for the default BGP instance.

peer-set-name: Specifies a BGP EPE peer set by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a peer set, this command displays information about all BGP EPE peer sets.

Examples

Display information about all BGP EPE peer sets.

```
<Sysname> display bgp egress-engineering peer-set
```

```
BGP egress peering segment peer-set: a
PeerSet label : 2172
Members: 0
```

```
BGP egress peering segment peer-set: b
PeerSet label : 5555
Members: 1
      BGP PeerNodeAdj : 3.3.3.3
```

```
BGP egress peering segment peer-set: c
PeerSet label: 65001
Label       : 65001
Members: 2
      BGP PeerNode: 1.1.1.1
      BGP PeerAdj : 10.1.1.1
```

```
PeerSet name: d
PeerSet label: 65002
Members: 2
      BGP PeerNode: 2.2.2.2
      BGP PeerAdj : 11.1.1.1
```

Table 7 Command output

Field	Description
BGP egress peering segment peer-set	Name of a BGP EPE peer set.
PeerSet label	SID used by the BGP EPE peer set.
Label	SID assigned to the BGP EPE peer set.
Members	Number of peers in the BGP EPE peer set.
BGP PeerNode	Address of the node peer.
BGP PeerAdj	Address of the adjacency peer.
BGP PeerNodeAdj	Address of the node-adjacency peer.

Modified command: peer egress-engineering

Use **peer egress-engineering** to enable BGP EPE for a peer or peer group and assign a label (SID) to the peer or peer group.

Use **undo peer egress-engineering** to restore the default for a peer or peer group.

Old syntax

```
peer { group-name | ipv4-address [ mask-length ] } egress-engineering [ adjacency | set ]  
[ route-policy policy-name ]
```

```
undo peer { group-name | ipv4-address [ mask-length ] } egress-engineering
```

New syntax

```
peer { group-name | ipv4-address [ mask-length ] } egress-engineering [ adjacency |  
node-adjacency | set ] [ label label-value | route-policy policy-name ]
```

```
undo peer { group-name | ipv4-address [ mask-length ] } egress-engineering
```

Views

BGP instance view

Change description

The following parameters were added:

node-adjacency: Assigns both a PeerNode SID and a PeerAdj SID.

label label-value: Specifies the SID value in the range of 16 to 1048575.

Modified command: display bgp egress-engineering ipv4

Use **display bgp egress-engineering ipv4** to display BGP EPE information.

Old syntax

```
display bgp [ instance instance-name ] egress-engineering ipv4 [ ipv4-address ]
```

New syntax

```
display bgp [ instance instance-name ] egress-engineering ipv4 [ ipv4-address ]  
[ verbose ]
```

Views

Any view

Change description

The **verbose** keyword was added.

verbose: Displays detailed BGP EPE information. If you do not specify this keyword, the command displays brief BGP EPE information.

New feature: SRv6 TE Policy CBTS

Configuring SRv6 TE policy CBTS

Prerequisites

Before configuring CBTS, you must create QoS traffic behaviors to mark the MPLS TE service class values for packets. For more information, see QoS configuration in *ACL and QoS Configuration Guide*.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 TE view.
traffic-engineering
4. Enter SRv6 TE policy view.
policy *policy-name*
5. Set a service class value for the SRv6 TE policy.
service-class *service-class-value*

By default, no service class value is set for an SRv6 TE policy. An SRv6 TE policy uses service class 255, which has the lowest forwarding priority.

Command reference

service-class

Use **service-class** to set a service class value for an SRv6 TE policy.

Use **undo service-class** to restore the default.

Syntax

service-class *service-class-value*

undo service-class

Default

No service class value is set for an SRv6 TE policy.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

service-class-value: Specifies a service class value in the range of 0 to 127. The smaller the service class value, the lower the SRv6 TE policy priority. An SRv6 TE policy that is not assigned a service class value has the lowest priority.

Usage guidelines

The device compares the service class value of the traffic with the service class values of SRv6 TE policies and forwards the traffic to a matching tunnel. The device uses the following rules to select an SRv6 TE policy to forward the traffic:

- If the traffic matches only one SRv6 TE policy, the device uses this SRv6 TE policy.
- If the traffic matches multiple SRv6 TE policies, the device selects an SRv6 TE policy based on the flow forwarding mode:
 - If there is only one flow and flow-based forwarding is used, the device randomly selects a matching SRv6 TE policy for packets of the flow.
 - If there are multiple flows or if there is one flow but packet-based forwarding is used, the device uses all matching SRv6 TE policies to load share the packets.

For more information about the flow identification and load sharing mode, see the **ip load-sharing mode** command.

- If the traffic does not match any SRv6 TE policy, the device randomly selects an SRv6 TE policy from all SRv6 TE policies with the smallest service class value.

To set a service class value for traffic, use the **remark service-class** command in traffic behavior view.

Examples

Set the service class value to 5 for SRv6 TE policy.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy 1
[Sysname-srv6-te-policy-1] service-class 5
```

Related commands

ip load-sharing mode (*Layer 3—IP Services Command Reference*)

remark service-class (*ACL and QoS Command Reference*)

New feature: Enabling the device to distribute SRv6 TE policy candidate path information to BGP-LS

Enabling the device to distribute SRv6 TE policy candidate path information to BGP-LS

About this task

After this feature is enabled, the device distributes SRv6 TE policy candidate path information to BGP-LS. BGP-LS advertises the SRv6 TE policy candidate path information in routes to meet application requirements.

Prerequisites

Before you configure this feature, enable the device to exchange LS information with the related peer or peer group. For more information about the LS exchange capability, see the BGP LS configuration in *Layer 3—IP Routing Configuration Guide*.

Procedure

1. Enter system view.
system-view
 2. Enter SRv6 view.
segment-routing ipv6
 3. Enter SRv6 TE view.
traffic-engineering
 4. Enable the device to distribute SRv6 TE policy candidate path information to BGP-LS.
distribute bgp-ls
- By default, the device cannot distribute SRv6 TE policy candidate path information to BGP-LS.

Command reference

distribute bgp-ls

Use **distribute bgp-ls** to enable the device to distribute SRv6 TE policy candidate path information to BGP-LS.

Use **undo distribute bgp-ls** to restore the default.

Syntax

distribute bgp-ls

undo distribute bgp-ls

Default

The device does not distribute SRv6 TE policy candidate path information to BGP-LS.

Views

SRv6 TE view

Predefined user roles

network-admin

Usage guidelines

After this command is executed, the device distributes SRv6 TE policy candidate path information to BGP-LS. BGP-LS advertises the SRv6 TE policy candidate path information in routes to meet application requirements.

Examples

Enable the device to distribute SRv6 TE policy candidate path information to BGP-LS.

```
<Sysname> system-view
```

```
[Sysname] segment-routing-ipv6
```

```
[Sysname-segment-routing-ipv6] traffic-engineering
```

```
[Sysname-srv6-te] distribute bgp-ls
```

New feature: SRv6 TE policy egress protection

Configuring SRv6 TE policy egress protection

Restrictions and guidelines for SRv6 TE policy egress protection configuration

To configure SRv6 TE policy egress protection, all nodes that the packets will traverse must support SRv6.

Configuring an End.M SID

Restrictions and guidelines

Perform this task on protection node for the egress node.

For more information about the commands used in this task, see IPv6 Segment Routing commands in *Segment Routing Command Reference*.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Create a locator and enter SRv6 locator view.
locator locator-name [ipv6-prefix ipv6-address prefix-length [args args-length | static static-length] *]
4. Configure an End.M SID and specify the locator to be protected by the End.M SID.
opcode opcode end-m mirror-locator ipv6-address prefix-length

Enabling egress protection

About this task

This task enables the SRv6 node to compute a backup path (mirror FRR path) for the egress node based on the End.M SID carried in a received IS-ISv6 or OSPFv3 route. When the egress node fails, the transit node can forward traffic to the node that protects the egress node according to the End.M SID.

In an egress protection scenario, the transit node deletes the mirror FRR path after completing route convergence. If the deletion occurs before the ingress node switches traffic back from the mirror FRR path, the traffic will be dropped because of no mirror FRR path.

To resolve this issue, you can configure a proper mirror FRR deletion delay time on the transit node to delay the deletion of the mirror FRR route. So, packets can be forwarded over the mirror FRR path before the ingress finishes the path switchover.

Enabling IS-IS egress protection

1. Enter system view.

system-view

2. Enter IS-IS view.
isis [*process-id*] [**vpn-instance** *vpn-instance-name*]
3. Enter IS-IS IPv6 address family view.
address-family ipv6 [**unicast**]
4. Enable IS-IS egress protection.
fast-reroute mirror enable
By default, IS-IS egress protection is disabled.
5. (Optional.) Configure the mirror FRR deletion delay time.
fast-reroute mirror delete-delay *delete-delay-time*
By default, the mirror FRR deletion delay time is 60 seconds.

Enabling OSPFv3 egress protection

1. Enter system view.
system-view
2. Enter OSPFv3 view.
ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enable OSPFv3 egress protection.
fast-reroute mirror enable
By default, OSPFv3 egress protection is disabled.
4. (Optional.) Configure the mirror FRR deletion delay time.
fast-reroute mirror delete-delay *delete-delay-time*
By default, the mirror FRR deletion delay time is 60 seconds.

Configuring the deletion delay time for remote SRv6 SID mappings with VPN instances/cross-connects/VSI

About this task

In an egress protection scenario, if the egress node and the egress node's protection node are disconnected, the protection node will delete the BGP routes received from the egress node. The remote SRv6 SID and VPN instance/cross-connect/VSI mappings will then be deleted as a result. To avoid this issue, you can configure the mappings deletion delay time on the protection node. This ensures that traffic is forwarded through the protection node before the ingress detects the egress failure and computes a new forwarding path.

Restrictions and guidelines

Perform this task on the protection node for the egress node.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Configure the deletion delay time for remote SRv6 SID mappings with VPN instances/cross-connects/VSI.
mirror remote-sid delete-delay *delete-delay-time*

By default, the deletion delay time for remote SRv6 SID and VPN instance/cross-connect/VSI mappings is 60 seconds.

Command reference

fast-reroute mirror delete-delay

Use **fast-reroute mirror delete-delay** to configure the mirror FRR deletion delay time.

Use **undo fast-reroute mirror delete-delay** to restore the default.

Syntax

fast-reroute mirror delete-delay *delete-delay-time*

undo fast-reroute mirror delete-delay

Default

The mirror FRR deletion delay time is 60 seconds.

Views

IS-IS IPv6 unicast address family view

OSPFv3 view

Predefined user roles

network-admin

Parameters

delete-delay-time: Specifies the deletion delay time, in the range of 1 to 21845 seconds.

Usage guidelines

In an egress protection scenario, the transit node deletes the mirror FRR path after completing route convergence. If the deletion occurs before the ingress node switches traffic back from the mirror FRR path, the traffic will be dropped because of no mirror FRR path.

To resolve this issue, you can configure a proper mirror FRR deletion delay time on the transit node to delay the deletion of the mirror FRR route. So, packets can be forwarded over the mirror FRR path before the ingress finishes the path switchover.

Examples

In IS-IS process 1, set the mirror FRR deletion delay time to 100 seconds.

```
<Sysname> system-view
```

```
[Sysname] isis 1
```

```
[Sysname-isis-1] address-family ipv6
```

```
[Sysname-isis-1-ipv6] fast-reroute mirror delete-delay 100
```

In OSPFv3 process 1, set the mirror FRR deletion delay time to 100 seconds.

```
<Sysname> system-view
```

```
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] fast-reroute mirror delete-delay 100
```

Related commands

fast-reroute mirror enable

fast-reroute mirror enable

Use **fast-reroute mirror enable** to enable egress protection.

Use **undo fast-reroute mirror enable** to disable egress protection.

Syntax

fast-reroute mirror enable

undo fast-reroute mirror enable

Default

Egress protection is disabled.

Views

IS-IS IPv6 unicast address family view

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

Egress protection enables an SRv6 node to compute a backup path (mirror FRR path) for the egress node based on the End.M SID carried in a received IPv6 IS-IS route or OSPFv3 route. When the egress node fails, the transit node can forward traffic to the node that protects the egress node according to the End.M SID.

Examples

Enable IS-IS egress protection.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] fast-reroute mirror enable
```

Enable OSPFv3 egress protection.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] fast-reroute mirror enable
```

mirror remote-sid delete-delay

Use **mirror remote-sid delete-delay** to configure the deletion delay time for remote SRv6 SID mappings with VPN instances/cross-connects/VSI.

Use **undo mirror remote-sid delete-delay** to restore the default.

Syntax

mirror remote-sid delete-delay *delete-delay-time*

undo mirror remote-sid delete-delay

Default

The deletion delay time for remote SRv6 SID and VPN instance/cross-connect/VSI mappings is 60 seconds.

Views

SRv6 view

Predefined user roles

network-admin

Parameters

delete-delay-time: Specifies the deletion delay time, in the range of 1 to 21845 seconds.

Usage guidelines

In an egress protection scenario, if the egress node and the egress node's protection node are disconnected, the protection node will delete the BGP routes received from the egress node. The remote SRv6 SID and VPN instance/cross-connect/VSI mappings will then be deleted as a result. To avoid this issue, you can configure the mappings deletion delay time on the protection node. This ensures that traffic is forwarded through the protection node before the ingress detects the egress failure and computes a new forwarding path.

Examples

Set the deletion delay time for remote SRv6 SID and VPN instance/cross-connect/VSI mappings to 100 seconds.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] mirror remote-sid delete-delay 100
```

display bgp mirror remote-sid

Use **display bgp mirror remote-sid** to display remote SRv6 SIDs protected by mirror SIDs.

Syntax

```
display bgp [ instance instance-name ] mirror remote-sid [ end-dt4 | end-dt46 | end-dt6 ] [ sid ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays information about the default instance.

end-dt4: Specifies remote SRv6 SIDs of the End.DT4 type.

end-dt46: Specifies remote SRv6 SIDs of the End.DT46 type.

end-dt6: Specifies remote SRv6 SIDs of the End.DT6 type.

sid: Specifies a remote SRv6 SID.

Usage guidelines

This command can display information about remote SRv6 SIDs protected by mirror SIDs on MPLS L3VPN over SRv6 or EVPN L3VPN over SRv6 networks.

If you do not specify any parameters, this command displays all remote SRv6 SIDs protected by mirror SIDs.

Examples

Display remote SRv6 SIDs protected by mirror SIDs on L3VPN over SRv6 networks.

```
<Sysname> display bgp mirror remote-sid
```

```
Remote SID: 3001::1:0:0
```

```
Remote SID type: End.DT4
```

```
Mirror locator: 3001::1/64
```

```
VPN instance name: vrf1
```

```
Remote SID: 3001::1:0:1
```

```
Remote SID type: End.DT6
```

```
Mirror locator: 3001::1/64
```

```
VPN instance name: vrf2
```

```
Remote SID: 1111:2222:3333:4444::1
```

```
Remote SID type: End.DT6
```

```
Mirror locator: 1111:2222:3333:4444:5555:6666:7777:8888/64
```

```
VPN instance name: vrf1
```

Table 8 Command output

Field	Description
Remote SID	Remote SRv6 SID.
Remote SID type	Type of the remote SRv6 SID: • End.DT4. • End.DT6. • End.DT46.
Mirror locator	IPv6 prefix and prefix length of the locator for the remote SRv6 SID.
VPN instance name	Name of the VPN instance associated with the remote SRv6 SID.
Remaining retention time	Remaining time before the mapping of the remote SRv6 SID and the VPN instance is deleted.

New feature: Enabling the device to drop traffic when an SRv6 TE policy becomes invalid

Enabling the device to drop traffic when an SRv6 TE policy becomes invalid

About this task

Enable this feature for an SRv6 TE policy if you want to use only the SRv6 TE policy to forward traffic.

By default, if all forwarding paths of an SRv6 TE policy become invalid, the device forwards the packets through IPv6 routing table lookup based on the packet destination IPv6 addresses.

After you execute the **drop-upon-invalid enable** command, the device drops the packets if all forwarding paths of the SRv6 TE policy become invalid.

Restrictions and guidelines

The **drop-upon-invalid enable** command does not take effect in the following cases:

- BSID request failed or BSID conflict occurred for the SRv6 TE policy. To view the BSID request state, see the **Request state** field in the **display segment-routing ipv6 te policy** command output.
- The SRv6 TE policy is invalid. To check the SRv6 TE policy validity, see the **Forwarding index** field in the **display segment-routing ipv6 te policy** command output. If the value is 0, the SRv6 TE policy is invalid.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6
3. Enter SRv6 TE view.
traffic-engineering
4. Enter SRv6 TE policy view.
policy policy-name
5. Enable the device to drop traffic when an SRv6 TE policy becomes invalid.
drop-upon-invalid enable

By default, the drop-upon-invalid feature is disabled for an SRv6 TE policy. The device does not drop traffic when the SRv6 TE policy becomes invalid.

Command reference

drop-upon-invalid enable

Use **drop-upon-invalid enable** to enable the device to drop traffic when an SRv6 TE policy becomes invalid.

Use **undo drop-upon-invalid enable** to disable the drop-upon-invalid feature for an SRv6 TE policy.

Syntax

drop-upon-invalid enable
undo drop-upon-invalid enable

Default

The drop-upon-invalid feature is disabled for an SRv6 TE policy. The device does not drop traffic when the SRv6 TE policy becomes invalid.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Usage guidelines

Enable this feature for an SRv6 TE policy if you want to use only the SRv6 TE policy to forward traffic.

By default, if all forwarding paths of an SRv6 TE policy become invalid, the device forwards the packets through IPv6 routing table lookup based on the packet destination IPv6 addresses.

After you execute the **drop-upon-invalid enable** command, the device drops the packets if all forwarding paths of the SRv6 TE policy become invalid.

The **drop-upon-invalid enable** command does not take effect in the following cases:

- BSID request failed or BSID conflict occurred for the SRv6 TE policy. To view the BSID request state, see the **Request state** field in the **display segment-routing ipv6 te policy** command output.
- The SRv6 TE policy is invalid. To check the SRv6 TE policy validity, see the **Forwarding index** field in the **display segment-routing ipv6 te policy** command output. If the value is 0, the SRv6 TE policy is invalid.

Examples

```
# Enable the device to drop traffic when SRv6 TE policy a1 becomes invalid.
```

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy a1
[Sysname-srv6-te-policy-a1] drop-upon-invalid enable
```

New feature: Automatic route advertisement for an SRv6 TE policy

Enabling automatic route advertisement for an SRv6 TE policy

About this task

As an SRv6 TE policy traffic steering mode, the automatic route advertisement mode advertises an SRv6 TE policy to IGP (IPv6 IS-IS or OSPFv3) for route computation, so as to forward the matching traffic through the SRv6 TE policy.

An SRv6 TE policy supports only automatic route advertisement in IGP shortcut mode, which is also called autoroute announce. Autoroute announce regards the SRv6 TE policy tunnel as a link that connects the tunnel ingress and egress. The tunnel ingress includes the SRv6 TE policy tunnel in IGP route computation.

With autoroute announce enabled on the tunnel ingress, only the tunnel ingress includes the SRv6 TE policy tunnel in IGP route computation. Because autoroute announce does not advertise the SRv6 TE policy tunnel as a link through IGP, other device will not include the SRv6 TE policy tunnel in route computation.

Procedure

1. Enter system view.
system-view
2. Enter SRv6 view.
segment-routing ipv6

3. Enter SRv6 TE view.
traffic-engineering
4. Enter SRv6 TE policy view.
policy *policy-name*
5. Enable automatic route advertisement for the SRv6 TE policy.
autoroute enable [**isis** | **ospfv3**]
By default, automatic route advertisement is disabled for an SRv6 TE policy.
6. Configure an autoroute metric for the SRv6 TE policy.
autoroute metric { **absolute** *value* | **relative** *value* }
By default, the autoroute metric of an SRv6 TE policy equals its IGP metric.
7. Return to system view.
quit
quit
quit
8. Include the SRv6 TE policy in IGP computation:
 - Execute the following commands in sequence to enable automatic route advertisement for IS-IS SRv6 TE policies.
isis [*process-id*] [**vpn-instance** *vpn-instance-name*]
address-family ipv6 [**unicast**]
srv6-policy autoroute enable [**level-1** | **level-2**]
By default, automatic route advertisement for SRv6 TE policies is disabled.

Command reference

autoroute enable

Use **autoroute enable** to enable automatic route advertisement for an SRv6 TE policy.

Use **undo autoroute enable** to disable automatic route advertisement for an SRv6 TE policy.

Syntax

autoroute enable [**isis** | **ospfv3**]

undo autoroute enable

Default

Automatic route advertisement is disabled for an SRv6 TE policy.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

isis: Enables automatic route advertisement for IPv6 IS-IS.

ospfv3: Enables automatic route advertisement for OSPFv3.

Usage guidelines

The automatic route advertisement feature advertises an SRv6 TE policy to IGP (IPv6 IS-IS or OSPFv3) for route computation.

An SRv6 TE policy supports only automatic route advertisement in IGP shortcut mode, which is also called autoroute announce. Autoroute announce regards the SRv6 TE policy tunnel as a link that connects the tunnel ingress and egress. The tunnel ingress includes the SRv6 TE policy tunnel in IGP route computation.

If you do not specify the **isis** or **ospfv3** keyword, both OSPFv3 and IPv6 IS-IS will include the SRv6 TE policy tunnel in route computation.

Examples

Enable automatic route advertisement for an SRv6 TE policy.

```
<Sysname> system-view
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy srv6policy
[Sysname-srv6-te-policy-srv6policy] autoroute enable
```

Related commands

autoroute metric

autoroute metric

Use **autoroute metric** to configure an autoroute metric for an SRv6 TE policy.

Use **undo autoroute metric** to restore the default.

Syntax

autoroute metric { **absolute value** | **relative value** }

undo autoroute metric

Default

The autoroute metric of an SRv6 TE policy equals its IGP metric.

Views

SRv6 TE policy view

Predefined user roles

network-admin

Parameters

absolute value: Specifies an absolute metric, an integer in the range of 1 to 65535.

relative value: Specifies a relative metric, an integer in the range of -10 to +10. The specified relative metric plus the IGP metric is the actual metric of the SRv6 TE policy.

Usage guidelines

After automatic route advertisement is enabled for an SRv6 TE policy, the policy is included in IGP route computation as a link. You can use this command to configure the metric of this link used for IGP route computation.

Examples

Set an absolute metric of 15 for SRv6 TE policy **srv6policy**.

```
<Sysname> system-view
```

```
[Sysname] segment-routing ipv6
[Sysname-segment-routing-ipv6] traffic-engineering
[Sysname-srv6-te] policy srv6policy
[Sysname-srv6-te-policy-srv6policy] autoroute metric absolute 15
```

Related commands

autoroute enable

srv6-policy autoroute enable

Use **srv6-policy autoroute enable** to enable automatic route advertisement for SRv6 TE policies.

Use **undo srv6-policy autoroute enable** to disable automatic route advertisement for SRv6 TE policies.

Syntax

srv6-policy autoroute enable [**level-1** | **level-2**]

undo srv6-policy autoroute enable

Default

Automatic route advertisement for SRv6 TE policies is disabled.

Views

IS-IS IPv6 address family view

Predefined user roles

network-admin

Parameters

level-1: Enables automatic route advertisement for Level-1 IS-IS SRv6 TE policies.

level-2: Enables automatic route advertisement for Level-2 IS-IS SRv6 TE policies.

Usage guidelines

This command advertises SRv6 TE policies to IGP (IPv6 IS-IS) for route computation.

If you do not specify the **level-1** or **level-2** keyword in IS-IS IPv6 address family view, this command enables automatic route advertisement for all levels of IS-IS SRv6 TE policies.

For this command to take effect on an SRv6 TE policy, you must also execute the **autoroute enable** command in the view of the SRv6 TE policy.

Examples

Enable automatic route advertisement for SRv6 TE policies of IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] srv6-policy autoroute enable
```

Related commands

autoroute enable

New feature: EVPN VPLS over SRv6/EVPN VPWS over SRv6

Configuring EVPN VPLS over SRv6

Configuring an EVPN instance

About this task

The BGP EVPN routes advertised by a PE carry the RD and route targets configured for the EVPN instance of the routes.

Procedure

1. Enter system view.

system-view

2. Enter VSI view.

vsi *vsi-name*

For more information about this command, see *EVPN Command Reference*.

3. Create an EVPN instance and enter VSI EVPN instance view.

evpn encapsulation srv6

4. Configure an RD for the EVPN instance.

route-distinguisher *route-distinguisher*

By default, no RD is configured for an EVPN instance.

For more information about this command, see *EVPN Command Reference*.

5. Configure route targets for the EVPN instance.

vpn-target { *vpn-target*<1–8> } [**both** | **export-extcommunity** | **import-extcommunity**]

By default, an EVPN instance does not have route targets.

For more information about this command, see *EVPN Command Reference*.

Parameter	Description
export-extcommunity	Do not specify the same export targets for the EVPN instances of different VSIs. Do not specify the same export targets for the EVPN instances created in different views (VSI view, VPN instance view, public instance view, and cross-connect group view). As a best practice, the export targets configured for the following objects do not match the import targets configured for the EVPN instances created in cross-connect group view: •VPN instances. •The public instance. •EVPN instances created in VSI view, VPN instance view, and public instance view.
import-extcommunity	As a best practice, the import targets configured for the following objects do not match the export targets configured for the EVPN instances created in cross-connect group view: •VPN instances.

Parameter	Description
	•The public instance. •EVPN instances created in VSI view, VPN instance view, and public instance view.

- (Optional.) Apply a tunnel policy to the EVPN instance.

tunnel-policy *tunnel-policy-name*

By default, no tunnel policy is applied to an EVPN instance.

For more information about this command, see *EVPN Command Reference*.

Configuring SRv6 SIDs

- Enter system view.

system-view

- Enable SRv6 and enter SRv6 view.

segment-routing ipv6

- Configure a locator and enter SRv6 locator view.

locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]

- Configure the opcode portion.

- Configure End.DT2U SIDs.

opcode { *opcode* | **hex** *hex-opcode* } **end-dt2u** **vsi** *vsi-name*

- Configure End.DT2UL SIDs.

opcode { *opcode* | **hex** *hex-opcode* } **end-dt2ul** **vsi** *vsi-name*

- Configure End.DX2 SIDs.

opcode { *opcode* | **hex** *hex-opcode* } **end-dx2** **vsi** *vsi-name* **interface** *interface-type* *interface-number*

- Configure End.DX2L SIDs.

opcode { *opcode* | **hex** *hex-opcode* } **end-dx2l** **vsi** *vsi-name* **interface** *interface-type* *interface-number*

- Configure End.DT2M SIDs.

opcode { *opcode* | **hex** *hex-opcode* } **end-dt2m** **vsi** *vsi-name*

Applying a locator to a VSI

About this task

Perform this task to allocate SRv6 SIDs from a locator to a VSI.

Procedure

- Enter system view.

system-view

- Enter VSI view.

vsi *vsi-name*

- Enter VSI EVPN instance view.

evpn encapsulation srv6

4. Apply a locator to the EVPN instance.

```
segment-routing ipv6 locator locator-name [ dt2u-locator dt2u-locator-name ]  
[ dt2ul-locator dt2ul-locator-name ] [ dx2-locator dx2-locator-name ] [ dx2l-locator  
dx2l-locator-name ] [ auto-sid-disable ]
```

By default, no locator is applied to a VSI.

Configuring unicast traffic forwarding based on End.DX2 and End.DX2L SIDs

About this task

By default, when a PE receives a packet that includes an End.DT2U or End.DT2UL SID, it looks up the MAC address table of the SID's VSI to forward the packet.

To improve forwarding efficiency, use this feature. This feature enables the PE to allocate an End.DX2 or End.DX2L SID to each AC associated with a VSI and advertise the SIDs to remote PEs through MAC/IP advertisement routes. When the PE receives an SRv6 packet that includes a locally allocated End.DX2 or End.DX2L SID, it does not look up the MAC address table. The PE directly forwards the packet to the AC that is associated with the SID after removing the SRv6 encapsulation.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enter VSI EVPN instance view.
evpn encapsulation srv6
4. Configure unicast traffic forwarding based on End.DX2 and End.DX2L SIDs.
unicast-forwarding dx2-based

By default, unicast traffic is forwarded based on End.DT2U and End.DT2UL SIDs.

Configuring the route recursion mode

About this task

After a PE receives a customer packet destined for an End.DT2M, End.DT2U, End.DT2UL, End.DX2, or End.DX2L SID, it forwards the packet according to the route recursion mode.

- **SRv6-BE mode**—In this mode, the PE first encapsulates the SID into the packet. Then, the PE searches the IPv6 routing table based on the SID encapsulated in the packet to forward the packet.
- **SRv6-TE mode**—In this mode, the PE first searches for a matching SRv6 TE policy based on the color attribute or next hop address of a matching route. Then, the PE adds an SRH to the packet. The SRH includes the End.DT2M, End.DT2U, End.DT2UL, End.DX2, or End.DX2L SID and the SID list of the SRv6 TE policy. Finally, the PE forwards the encapsulated packet through the SRv6 TE policy. For more information, see "Configuring SRv6 TE policies."
- **SRv6-TE and SRv6-BE hybrid mode**—In this mode, the PE preferentially uses the SRv6-TE mode to forward the packet. If no SRv6 TE policy is available for the packet, the PE forwards the packet in SRv6-BE mode.

Procedure

1. Enter system view.
system-view

2. Enter VSI view.
vsi *vsi-name*
 3. Enter VSI EVPN instance view.
evpn encapsulation srv6
 4. Configure the route recursion mode.
segment-routing ipv6 { **best-effort** | **traffic-engineering** [**best-effort**] }
- By default, a PE searches the IPv6 routing table based on the next hop of a matching EVPN route to forward traffic.

Configuring color-based traffic steering

About this task

The device searches for an SRv6 TE policy that has the same color and endpoint address as the color and next hop address of a BGP EVPN route. If a matching SRv6 TE policy exists, the device recurses the route to that SRv6 TE policy. When the device receives packets that match the route, it forwards the packets through the SRv6 TE policy.

Use one of the following methods to configure colors for BGP EVPN routes:

- **Routing policy-based coloring**—Configure a routing policy to add the color extended community attribute to BGP EVPN routes or modify the existing color extended community attribute in BGP EVPN routes.
- **Default color**—Specify a color as the default color for BGP EVPN routes. A BGP EVPN route uses the default color for color-based traffic steering if the route does not have the color extended community attribute or match a routing policy to obtain a color.

Restrictions and guidelines

Traffic steering is based on the greatest value among the color extended community attributes when the following conditions exist:

- You specify the **additive** keyword for the **apply extcommunity color** clause in a routing policy, and specify the routing policy for the **import route-policy** command.
- The received BGP EVPN routes carry the color extended community attribute.

Configuring routing policy-based coloring

1. Enter system view.
system-view
2. Enter routing policy node view.
route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*
For more information about this command, see routing policy commands in *Layer 3—IP Routing Command Reference*.
3. Set the color extended community attribute for BGP routes.
apply extcommunity color *color* [**additive**]
By default, no color extended community attribute is set for BGP routes.
For more information about this command, see routing policy commands in *Layer 3—IP Routing Command Reference*.
4. Return to system view.
quit
5. Enter VSI view.
vsi *vsi-name*
6. Enter VSI EVPN instance view.

evpn encapsulation srv6

7. Apply the routing policy as an import policy to the EVPN instance.

import route-policy route-policy

By default, no import routing policy is applied to an EVPN instance. The EVPN instance does not filter received routes.

8. Apply the routing policy as an export policy to the EVPN instance.

export route-policy route-policy

By default, no export routing policy is applied to an EVPN instance. The EVPN instance does not filter advertised routes.

Configuring the default color for BGP EVPN routes

1. Enter system view.

system-view

2. Enter VSI view.

vsi vsi-name

3. Enter VSI EVPN instance view.

evpn encapsulation srv6

4. Configure the default color for BGP EVPN routes.

default color color-value

By default, no default color is configured for BGP EVPN routes.

Configuring PEs to exchange BGP EVPN routes

Restrictions and guidelines

For more information about BGP commands, see *Layer 3—IP Routing Command Reference*.

Procedure

1. Enter system view.

system-view

2. Enter BGP instance view.

bgp as-number [instance instance-name]

3. Configure an IPv6 peer or peer group.

peer { group-name | ipv6-address [prefix-length] } as-number as-number

4. Specify the source interface of TCP connections to a peer or peer group.

peer { group-name | ipv6-address [prefix-length] } connect-interface interface-type interface-number

By default, BGP uses the IPv6 address of the output interface in the optimal route to the BGP peer or peer group as the source address of TCP connections to the peer or peer group.

5. Enter BGP EVPN address family view.

address-family l2vpn evpn

6. Enable BGP to exchange EVPN routes with an IPv6 peer or peer group.

peer { group-name | ipv6-address [prefix-length] } enable

By default, BGP cannot exchange EVPN routes with an IPv6 peer or peer group.

7. Enable BGP to advertise SRv6-encapsulated EVPN routes to a peer or peer group.

peer { group-name | ipv6-address [prefix-length] } advertise encap-type srv6

By default, BGP advertises VXLAN-encapsulated EVPN routes to a peer or peer group.

Configuring SRv6 PW packet statistics

About this task

This task enables the packet statistics feature for all SRv6 PWs in a VSI EVPN instance.

To display inbound packet statistics for all SRv6 PWs, use the **display l2vpn statistics srv6-pw inbound** command.

To display outbound packet statistics for each SRv6 PW, use the **display l2vpn peer srv6 verbose** command.

To clear SRv6 PW packet statistics, use the **reset l2vpn statistics srv6-pw** command.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi vsi-name
3. Enter VSI EVPN instance view.
evpn encapsulation srv6
4. Enable SRv6 PW packet statistics.
statistics enable

By default, SRv6 PW packet statistics is disabled.

Using ping to test the connectivity of an SRv6 PW

About this task

In an EVPN VPLS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Perform this task to test the connectivity of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs.

The test process is as follows:

1. The local PE constructs an MPLS echo request packet and searches for the SRv6 tunnel that matches the specified VSI. After obtaining the End.DT2U SID of the SRv6 tunnel, the PE adds a UDP header and an IPv6 header to the packet and forwards the packet to the remote PE.
2. Upon receiving the MPLS echo request packet, the remote PE replies to the request packet.
3. The local PE identifies the connectivity of the SRv6 PW based on whether it has received MPLS echo reply packets from the remote PE and the reply response time. In addition, the local PE outputs statistics about the ping operation.

Procedure

To test the connectivity of an SRv6 PW from the local PE to the remote PE in an EVPN VPLS over SRv6 network, execute the following command in any view:

ping evpn vpls srv6 vsi vsi-name mac mac-address [**-a** source-ipv6 | **-c** count | **-h** hop-limit | **-m** interval | **-r** reply-mode | **-s** packet-size | **-t** time-out | **-tc** tc] *

Using tracert to test the connectivity of an SRv6 PW

About this task

In an EVPN VPLS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Perform this task to trace the path of the SRv6 PW from the local PE to the remote PE when

packet loss or traffic interruption occurs between the PEs. This task helps you locate the failed nodes on the path.

The test process is as follows:

1. The local PE constructs an MPLS echo request packet and searches for the SRv6 tunnel that matches the specified VSI. After obtaining the End.DT2U SID of the SRv6 tunnel, the PE adds a UDP header and an IPv6 header to the packet and forwards the packet to the remote PE. In the IPv6 header, the value of the **Hop limit** field is set to 1.
2. When the next node receives the packet, the value of the **Hop limit** field changes to 0. Then, the node sends an ICMPv6 timeout packet to the first node (the local PE).
3. When the local PE receives the ICMPv6 timeout packet, it increases the value of the **Hop limit** field by one in the MPLS echo request packet. Then, the local PE forwards the request packet to the remote PE. The value of the **Hop limit** field is 2.
4. The value of the **Hop limit** field decreases by one each time the request packet reaches a node. When the value of the **Hop limit** field decreases to 0, the node that receives the request packet responds to the first node with an ICMPv6 timeout packet. If the node that receives the request packet is the destination node, it sends an MPLS echo reply packet to the first node.
5. The local PE repeats the previous step until one of the following conditions exist:
 - The local PE has not received any reply packets before the reply timeout time expires for all request packets.
 - The local PE receives a reply packet from the remote PE.
6. The local PE identifies the connectivity of the SRv6 PW based on whether it has received MPLS echo reply packets from the remote PE and the reply response time. In addition, the local PE outputs statistics about the tracer operation.

Procedure

To trace the path of an SRv6 PW from the local PE to the remote PE in an EVPN VPLS over SRv6 network, execute the following command in any view:

```
tracert evpn vpls srv6 vsi vsi-name mac mac-address [ -a source-ip | -h hop-limit | -r reply-mode | -t time-out | -tc tc ] *
```

Configuring EVPN VPWS over SRv6

Configuring a cross-connect group and its EVPN instance

1. Enter system view.
system-view
2. Create a cross-connect group and enter its view.
xconnect-group *group-name*
For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.
3. (Optional.) Configure a description for the cross-connect group.
description *text*
By default, no description is configured for a cross-connect group.
For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.
4. (Optional.) Bring the cross-connect group.
undo shutdown

By default, a cross-connect group is not administratively down.

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

5. Create an EVPN instance for the cross-connect group and enter its view.

evpn encapsulation srv6

6. Configure an RD for the EVPN instance.

route-distinguisher route-distinguisher

By default, no RD is configured for the EVPN instance of a cross-connect group.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

7. Configure route targets for the EVPN instance.

vpn-target { vpn-target<1-8> } [both | export-extcommunity | import-extcommunity]

By default, no route targets are configured for the EVPN instance of a cross-connect group.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

Parameter	Description
export-extcommunity	Do not specify the same export targets for the EVPN instances of different cross-connect groups. Do not specify the same export targets for the EVPN instances of a cross-connect group and a VSI. As a best practice, the export targets of the EVPN instance of a cross-connect group do not match the import targets configured in VPN instance view, VPN instance EVPN view, public instance view, public instance EVPN view, or VSI EVPN instance view.
import-extcommunity	As a best practice, the import targets of the EVPN instance of a cross-connect group do not match the export targets configured in VPN instance view, VPN instance EVPN view, public instance view, public instance EVPN view, or VSI EVPN instance view.

8. Return to cross-connect group view.

quit

9. Create a cross-connect and enter its view.

connection connection-name

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

Configuring SRv6 SIDs

Restrictions and guidelines

For more information about the commands in this section, see SRv6 commands in *Segment Routing Command Reference*.

Procedure

1. Enter system view.

system-view

2. Enable SRv6 and enter SRv6 view.

segment-routing ipv6

3. Configure a locator and enter SRv6 locator view.
locator *locator-name* [**ipv6-prefix** *ipv6-address prefix-length* [**args** *args-length* | **static** *static-length*] *]
4. Configure an opcode for End.DX2 SIDs.
opcode { *opcode* | **hex** *hex-opcode* } **end-dx2** **xconnect-group** *group-name*
connection *connection-name*
5. (Optional.) Configure an opcode for End.DX2L SIDs.
opcode { *opcode* | **hex** *hex-opcode* } **end-dx2l** **xconnect-group** *group-name*
connection *connection-name*
 Use this command only in the bypass PW network.

Applying a locator to a cross-connect

About this task

Perform this task to apply a locator to a cross-connect for the cross-connect to apply for End.DX2 and End.DX2L SIDs from the locator.

Procedure

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter cross-connect view.
connection *connection-name*
4. Apply a locator to the cross-connect.
segment-routing ipv6 locator *locator-name* [**dx2l-locator** *dx2l-locator-name*]
 [**auto-sid-disable**]
 By default, no locator is applied to a cross-connect.
5. Create an SRv6 PW and enter SRv6 PW view.
evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
 [**tunnel-policy** *tunnel-policy-name*]
 For more information about this command, see EVPN commands in *EVPN Command Reference*.

Configuring the route recursion mode

About this task

After a PE receives a customer packet destined for an End.DX2 or End.DX2L SID, it forwards the packet according to the route recursion mode.

- **SRv6-BE mode**—This mode is also called SID-based forwarding mode. In this mode, the PE first encapsulates the End.DX2 or End.DX2L SID into the packet. Then, the PE searches the IPv6 routing table based on the End.DX2 or End.DX2L SID encapsulated in the packet to forward the packet.
- **SRv6-TE mode**—This mode is also called SRv6 TE policy-based forwarding mode. In this mode, the PE first searches for a matching SRv6 TE policy based on the packet attributes. Then, the PE adds an SRH to the packet. The SRH includes the End.DX2 or End.DX2L SID and the SID list of the SRv6 TE policy. Finally, the PE forwards the encapsulated packet through the SRv6 TE policy. For more information, see "Configuring SRv6 TE policies."

- **SRv6-TE and SRv6-BE hybrid mode**—In this mode, the PE preferentially uses the SRv6-TE mode to forward the packet. If no SRv6 TE policy is available for the packet, the PE forwards the packet in SRv6-BE mode.

Prerequisites

To use the SRv6-TE mode or the SRv6-TE and SRv6-BE hybrid mode, you must configure a tunnel policy and SRv6 TE policy. For more information, see tunnel policy configuration in *MPLS Configuration Guide* and "Configuring SRv6 TE policies."

Procedure

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter cross-connect group EVPN instance view.
evpn encapsulation srv6
4. Configure the route recursion mode.
segment-routing ipv6 { best-effort | traffic-engineering | traffic-engineering best-effort }

By default, a PE searches the IPv6 routing table based on the next hop of a matching EVPN route to forward traffic.

Configuring color-based traffic steering

About this task

The device searches for an SRv6 TE policy that has the same color and endpoint address as the color and next hop address of a BGP EVPN route. If a matching SRv6 TE policy exists, the device recurses the route to that SRv6 TE policy. When the device receives packets that match the route, it forwards the packets through the SRv6 TE policy.

Use one of the following methods to configure colors for BGP EVPN routes:

- **Routing policy-based coloring**—Configure a routing policy to add the color extended community attribute to BGP EVPN routes or modify the existing color extended community attribute in BGP EVPN routes.
- **Default color**—Specify a color as the default color for BGP EVPN routes. A BGP EVPN route uses the default color for color-based traffic steering if the route does not have the color extended community attribute or match a routing policy to obtain a color.

Restrictions and guidelines

Traffic steering is based on the greatest value among the color extended community attributes when the following conditions exist:

- You specify the **additive** keyword for the **apply extcommunity color** clause in a routing policy, and specify the routing policy for the **import route-policy** command.
- The received BGP EVPN routes carry the color extended community attribute.

Configuring routing policy-based coloring

1. Enter system view.
system-view
2. Enter routing policy node view.
route-policy *route-policy-name* { **deny** | **permit** } **node** *node-number*

For more information about this command, see routing policy commands in *Layer 3—IP Routing Command Reference*.

3. Set the color extended community attribute for BGP routes.

apply extcommunity color *color* [**additive**]

By default, no color extended community attribute is set for BGP routes.

For more information about this command, see routing policy commands in *Layer 3—IP Routing Command Reference*.

4. Return to system view.

quit

5. Enter cross-connect group view.

xconnect-group *group-name*

6. Enter EVPN instance view of the cross-connect group.

evpn encapsulation srv6

7. Apply the routing policy as an export policy to the EVPN instance.

export route-policy *route-policy*

By default, no export routing policy is applied to an EVPN instance. The EVPN instance does not filter advertised routes.

For more information about this command, see *EVPN Command Reference*.

8. Apply the routing policy as an import policy to the EVPN instance.

import route-policy *route-policy*

By default, no import routing policy is applied to an EVPN instance. The EVPN instance does not filter received routes.

For more information about this command, see *EVPN Command Reference*.

Configuring the default color for BGP EVPN routes

1. Enter system view.

system-view

2. Enter cross-connect group view.

xconnect-group *group-name*

3. Enter EVPN instance view of the cross-connect group.

evpn encapsulation srv6

4. Configure the default color for BGP EVPN routes.

default color *color-value*

By default, no default color is configured for BGP EVPN routes.

Configuring tunnel policy-based traffic steering

About this task

The device searches the tunnel policies for a matching SRv6 TE policy based on the next hop of a matching route. Configure a preferred tunnel or load sharing tunnel policy that uses the SRv6 TE policy. In this way, the SRv6 TE policy will be used as the public tunnel to carry the SRv6 PW that forwards the packets of private network packets. For more information about tunnel policies, see *MPLS Configuration Guide*.

Configuring a tunnel policy

1. Enter system view.

system-view

2. Create a tunnel policy and enter tunnel policy view.
tunnel-policy *tunnel-policy-name* [**default**]
 3. Configure the tunnel policy. Choose a minimum of one option:
 - Specify an SRv6 TE policy as a preferred tunnel of the tunnel policy.
preferred-path srv6-policy { **name** *srv6-policy-name* | **end-point ipv6** *ipv6-address* **color** *color-value* }
By default, no preferred tunnel is specified for a tunnel policy.
 - Configuring SRv6 TE policy load sharing for the tunnel policy.
select-seq srv6-policy load-balance-number *number*
By default, no load sharing tunnel policy is configured.
- For more information about the tunnel policy commands, see *MPLS Command Reference*.

Specifying the tunnel policy for a PW

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter cross-connect view.
connection *connection-name*
4. Create an SRv6 PW and specify a tunnel policy for this PW.
evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
tunnel-policy *tunnel-policy-name*

Configuring PEs to exchange BGP EVPN routes

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Configure an IPv6 peer or peer group.
peer { *group-name* | *ipv6-address* [*prefix-length*] } **as-number** *as-number*
For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.
4. Specify the source interface of TCP connections to a peer or peer group.
peer { *group-name* | *ipv6-address* [*prefix-length*] } **connect-interface** *interface-type* *interface-number*
By default, BGP uses the IPv6 address of the output interface in the optimal route to the BGP peer or peer group as the source address of TCP connections to the peer or peer group.
For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.
5. Enter BGP EVPN address family view.
address-family l2vpn evpn
For more information about this command, see *EVPN Command Reference*.
6. Enable BGP to exchange EVPN routes with an IPv6 peer or peer group.
peer { *group-name* | *ipv6-address* [*prefix-length*] } **enable**

By default, BGP cannot exchange EVPN routes with an IPv6 peer or peer group.

For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.

7. Enable BGP to advertise SRv6-encapsulated BGP EVPN routes to a peer or peer group.

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise encap-type srv6**

By default, BGP advertises VXLAN-encapsulated BGP EVPN routes to a peer or peer group.

Configuring LDP PWs as ACs for SRv6 PWs

Restrictions and guidelines

The data encapsulation type of an LDP PW must be the same as the access mode of the ACs mapped to the same cross-connect as the LDP PW. If they are different, perform one of the following tasks:

- Use the **pw-type** command on the PW class to which the LDP PW belongs to change the PW data encapsulation type.
- Use the **ac interface** command for the ACs and specify the **access-mode** parameter in the command to change the access mode of the ACs.

Procedure

1. Enter system view.

system-view

2. Enter cross-connect group view.

xconnect-group *group-name*

3. Enter cross-connect group EVPN instance view.

evpn encapsulation srv6

4. Return to cross-connect group view.

quit

5. Enter cross-connect view.

connection *connection-name*

6. Create an LDP PW for the cross-connect and enter cross-connect PW view.

peer *ip-address* **pw-id** *pw-id* [**ignore-standby-state**] [**admin** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

The LDP PW configured by using this command is an UPW, which acts as an AC for the EVPN VPWS over SRv6 network.

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

7. (Optional.) Assign an ESI to the UPW.

esi *esi-id*

By default, no ESI is assigned to an UPW.

At a multihomed site, use this command on the PEs in the MPLS L2VPN and EVPN VPWS over SRv6 networks.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

8. (Optional.) Set the redundancy mode of the UPW.

evpn redundancy-mode { **all-active** | **single-active** }

By default, the redundancy mode is all-active.

At a multihomed site, use this command on the PEs in the MPLS L2VPN and EVPN VPWS over SRv6 networks.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

9. Configure a backup LDP PW for the cross-connect and enter cross-connect backup PW view.

backup-peer *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

At a multihomed site, use this command on the multihomed PEs.

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

10. Return to cross-connect view.

quit

quit

11. Create an SRv6 PW and enter SRv6 PW view.

evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
[**tunnel-policy** *tunnel-policy-name*]

For more information about this command, see *EVPN Command Reference*.

Configuring static PWs as ACs for SRv6 PWs

1. Enter system view.

system-view

2. Enter cross-connect group view.

xconnect-group *group-name*

3. Enter cross-connect group EVPN instance view.

evpn encapsulation srv6

4. Return to cross-connect group view.

quit

5. Enter cross-connect view.

connection *connection-name*

6. Create a static PW for the cross-connect and enter cross-connect PW view.

peer *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value* [**admin** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

The static PW configured by using this command is an UPW, which acts as an AC for the EVPN VPWS over SRv6 network.

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

7. (Optional.) Assign an ESI to the UPW.

esi *esi-id*

By default, no ESI is assigned to an UPW.

At a multihomed site, use this command on the PEs in the MPLS L2VPN and EVPN VPWS over SRv6 networks.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

8. (Optional.) Set the redundancy mode of the UPW.

evpn redundancy-mode { **all-active** | **single-active** }

By default, the redundancy mode is all-active.

At a multihomed site, use this command on the PEs in the MPLS L2VPN and EVPN VPWS over SRv6 networks.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

9. Configure a backup static PW for the cross-connect and enter cross-connect backup PW view.

backup-peer *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value*
[**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

At a multihomed site, use this command on the multihomed PEs.

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

10. Return to cross-connect view.

quit

quit

11. Create an SRv6 PW and enter SRv6 PW view.

evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
[**tunnel-policy** *tunnel-policy-name*]

For more information about this command, see *EVPN Command Reference*.

Configuring SRv6 PW packet statistics

About this task

When SRv6 PW packet statistics is enabled, you can use the **display l2vpn peer srv6 verbose** command to display SRv6 PW packet statistics. To clear SRv6 PW packet statistics, use the **reset l2vpn statistics srv6-pw** command.

Procedure

1. Enter system view.

system-view

2. Enter cross-connect group view.

xconnect-group *group-name*

3. Enter cross-connect view.

connection *connection-name*

4. Enter SRv6 PW view.

evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
[**tunnel-policy** *tunnel-policy-name*]

5. Enable SRv6 PW packet statistics.

statistics enable

By default, SRv6 PW packet statistics is disabled.

Using ping to test the connectivity of an SRv6 PW

About this task

In an EVPN VPWS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Perform this task to test the connectivity of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs.

The test process is as follows:

1. The local PE constructs an MPLS echo request packet and searches for the SRv6 tunnel that matches the specified cross-connect group name, local service ID, and remote service ID. After obtaining the End.DX2 SID of the SRv6 tunnel, the PE adds a UDP header and an IPv6 header to the packet and forwards the packet to the remote PE.
2. Upon receiving the MPLS echo request packet, the remote PE replies to the request.
3. The local PE identifies the connectivity of the SRv6 PW based on whether it has received MPLS echo replies from the remote PE and the reply response time. In addition, the local PE outputs statistics about the ping operation.

Procedure

To test the connectivity of an SRv6 PW from the local PE to the remote PE in an EVPN VPWS over SRv6 network, execute the following command in any view:

```
ping evpn vpws srv6 xconnect-group group-name local-service-id remote-service-id [ -a source-ipv6 | -c count | -h hop-limit | -m interval | -r reply-mode | -s packet-size | -t time-out | -tc tc ] *
```

Using tracer to test the connectivity of an SRv6 PW

About this task

In an EVPN VPWS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Perform this task to trace the path of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs. This task helps you locate the failed nodes on the path.

The test process is as follows:

1. The local PE constructs an MPLS echo request packet and searches for the SRv6 tunnel that matches the specified cross-connect group name, local service ID, and remote service ID. After obtaining the End.DX2 SID of the SRv6 tunnel, the PE adds a UDP header and an IPv6 header to the packet and forwards the packet to the remote PE. In the IPv6 header, the value of the **Hop limit** field is set to 1.
2. When the next node receives the packet, the value of the **Hop limit** field changes to 0. Then, the node sends an ICMPv6 timeout packet to the first node (the local PE).
3. When the local PE receives the ICMPv6 timeout packet, it increases the value of the **Hop limit** field by one in the MPLS echo request packet. Then, the local PE forwards the request packet to the remote PE. The value of the **Hop limit** field is 2.
4. The value of the **Hop limit** field decreases by one each time the request packet reaches a node. When the value of the **Hop limit** field decreases to 0, the node that receives the request packet responds to the first node with an ICMPv6 timeout packet. If the node that receives the request packet is the destination node, it sends an MPLS echo reply packet to the first node.
5. The local PE repeats the previous step until one of the following conditions exist:
 - The local PE has not received any reply packets before the reply timeout time expires for all request packets.
 - The local PE receives a reply packet from the remote PE.
6. The local PE identifies the connectivity of the SRv6 PW based on whether it has received MPLS echo reply packets from the remote PE and the reply response time. In addition, the local PE outputs statistics about the tracer operation.

Procedure

To trace the path of an SRv6 PW from the local PE to the remote PE in an EVPN VPWS over SRv6 network, execute the following command in any view:

```
tracer evpn vpws srv6 xconnect-group group-name local-service-id remote-service-id [ -a source-ip | -h hop-limit | -r reply-mode | -t time-out | -tc tc ] *
```


Command reference

display l2vpn statistics srv6-pw inbound

Use **display l2vpn statistics srv6-pw inbound** to display incoming packet statistics for SRv6 PWs in an EVPN VPLS over SRv6 network.

Syntax

display l2vpn statistics srv6-pw inbound [**vsi** *vsi-name*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VSI, this command displays incoming packet statistics for all SRv6 PWs on all VSIs.

Usage guidelines

Use this command to display incoming packet statistics for all SRv6 PWs on the specified VSI or all VSIs.

To display outgoing packet statistics, use the **display l2vpn peer srv6 verbose** command.

Examples

Display incoming packet statistics for all SRv6 PWs on VSI **aaa**.
<Sysname> display l2vpn statistics srv6-pw inbound vsi aaa

```
VSI name: aaa
Input statistics:
  Octets           : 0
  Packets          : 0
  Errors           : 0
  Discards         : 0
Input rate       :
  Bytes per second : 0
  Packets per second : 0
```

Table 9 Command output

Field	Description
Input statistics	Incoming packet statistics for all SRv6 PWs: • Octets—Number of incoming bytes. • Packets—Number of incoming packets. • Errors—Number of error packets. • Discards—Number of discarded packets.
Input rate	Incoming traffic rate for all SRv6 PWs: • Bytes per second—Number of incoming bytes per second. • Packets per second—Number of incoming packets per second.

Related commands

reset l2vpn statistics srv6-pw
statistics enable

display l2vpn xconnect-group

Use **display l2vpn xconnect-group** to display L2VPN cross-connect group information.

Syntax

display l2vpn xconnect-group [**evpn-srv6** | **name** *group-name*] [**connection** *connection-name*] [**count** | **verbose**]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

evpn-srv6: Specifies cross-connect groups in the EVPN VPWS over SRv6 network.

name *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters.

connection *connection-name*: Specifies a cross-connect by its name, a case-sensitive string of 1 to 20 characters. The cross-connect name cannot contain hyphens (-). If you do not specify a cross-connect, this command displays information about all cross-connects in the specified cross-connect group.

count: Displays cross-connect group statistics.

verbose: Displays detailed cross-connect group information.

Examples

Display brief information about all cross-connect groups in the EVPN VPWS over SRv6 network.

```
<Sysname> display l2vpn xconnect-group evpn-srv6
```

Status Codes: UP - Up, DN - Down, DF - Defect, BD - Blocked, AD - Admin Down,
DL - Idle, DP - Duplicate

Total number of cross-connections: 1, 1 up, 0 down, 0 admin down

Xconnect-group	Connection	ST
Segment1	ST Segment2	ST

vpna	pw1	UP
GE1/0/2	UP EVPN 2::2	UP

Display statistics about all cross-connect groups in the EVPN VPWS over SRv6 network.

```
<Sysname> display l2vpn xconnect-group evpn-srv6 count
```

Status Codes: UP - Up, DN - Down, DF - Defect, BD - Blocked, AD - Admin Down,
DL - Idle, DP - Duplicate

Total number of cross-connections: 1, 1 up, 0 down, 0 admin down

Table 10 Command output

Field	Description
ST	State of the cross-connect: UP—The cross-connect is up. DN—The cross-connect is down. AD—The cross-connect is manually shut down by using the shutdown command.
Segment1 / Segment2	For an AC segment: - If the AC is a Layer 3 interface, this field displays the interface name. - If the AC is an Ethernet service instance, this field displays the Ethernet service instance name. For an SRv6 tunnel segment, this field displays the establishment method of the SRv6 tunnel and the IPv6 address of the remote PE. Only the EVPN establishment method is supported.
ST	If this field displays AC state, the following options are available: UP—The AC is up. DN—The AC is down. If this field displays SRv6 tunnel state, the following options are available: UP—The tunnel is up. DN—The tunnel is down. DF—BFD detects that the tunnel has defects. BD—The tunnel is a backup tunnel. Its tunnel interface is up, but the tunnel is blocked because the primary tunnel is operating correctly. DL—The input SID of the tunnel is not available. DP—This option is not supported in the current software version.

Display detailed information about all cross-connect groups in the EVPN VPWS over SRv6 network.

```
<Sysname> display l2vpn xconnect-group evpn-srv6 verbose
```

```
Xconnect-group Name: vpna
```

```

Connection Name      : pw1
Connection ID        : 1
State                : Up
MTU                  : 1500
PW Redundancy Mode   : Slave
Diffserv Mode        : -

```

```
SRv6 tunnels:
```

```

Peer      : 2::2
Link ID    : 0x1
State      : Up

```

```
ACs:
```

AC	Link ID	State
GE1/0/1	0x0	Up

```
Statistics: Disabled
```

Display detailed information about all cross-connect groups in the EVPN VPWS over SRv6 network.

```
<Sysname> display l2vpn xconnect-group evpn-srv6 verbose
```

```
Xconnect-group Name: vpna
```

```
Connection Name      : pw1
Connection ID        : 1
State                : Up
MTU                  : 1500
PW Redundancy Mode   : Slave
Diffserv Mode        : -
```

```
SRv6 tunnels:
```

```
Peer                : 2::2
Link ID              : 0x1
State                : Up
```

```
ACs:
```

```
AC                      Link ID  State
GE1/0/4 srv1            0x0      Up
```

```
Statistics: Disabled
```

Table 11 Command output

Field	Description
Description	Description of the cross-connect group. If no description is configured, this field is not available.
State	Cross-connect group state: Up—The cross-connect group is up. Down—The cross-connect group is down. Administratively down—The cross-connect group is manually shut down by using the shutdown command.
MTU	Maximum transmission unit of cross-connects.
PW Redundancy Mode	PW redundancy operation mode: Slave—Master/slave mode and the local PE operates as the slave node. Master—Master/slave mode and the local PE operates as the master node. Independent—Independent mode.
Diffserv Mode	DiffServ mode. Options include the following: ingress—DiffServ mode for the inbound direction. egress—DiffServ mode for the outbound direction. pipe—Pipe mode. short-pipe—Short-pipe mode. uniform—Uniform mode trust—Priority trust mode inner-dot1p—Trusts the inner 802.1p priority in packets. dscp—Trusts the DSCP in packets. af1, af2, af3, af4, be, cs6, cs7, or ef represents the MPLS EXP value. If no DiffServ mode is configured, this field displays a hyphen (-).
SRv6 tunnels	SRv6 tunnel information.
Peer	IPv6 address of the SRv6 tunnel remote PE.

Field	Description
Link ID	Link ID of the SRv6 tunnel on the cross-connect.
State	SRv6 tunnel state, which can be Up , Down , Blocked , or Defect .
ACs	AC information.
AC	For a Layer 3 interface, this field displays the interface name. For an Ethernet service instance, this field displays the name of the Ethernet service instance and the name of the Layer 2 interface where the Ethernet service instance name resides.
Link ID	Link ID of the AC on the cross-connect.
State	AC state, which can be Up or Down .
Statistics	AC packet statistics state.

evpn encapsulation srv6

Use **evpn encapsulation srv6** to create an EVPN instance, specify it to use SRv6 encapsulation, and enter its view, or enter the view of an existing EVPN instance that uses SRv6 encapsulation.

Use **undo evpn encapsulation** to restore the default.

Syntax

```
evpn encapsulation srv6
undo evpn encapsulation
```

Default

No EVPN instance is created.

Views

VSI view
Cross-connect group view

Predefined user roles

network-admin

Usage guidelines

Before you can configure EVPN settings for a VSI or cross-connect group, you must create an EVPN instance on it.

This command is mutually exclusive with the **evpn encapsulation binding instance** command. You cannot use them together on the same VSI.

Examples

Create an EVPN instance and specify it to use SRv6 encapsulation on VSI **aaa** and enter its view.

```
<Sysname> system-view
[Sysname] vsi aaa
[Sysname-vsi-aaa] evpn encapsulation srv6
[Sysname-vsi-aaa-evpn-srv6]
```

export route-policy

Use **export route-policy** to apply an export routing policy to an EVPN instance.

Use **undo export route-policy** to restore the default.

Syntax

export route-policy *route-policy*
undo export route-policy

Default

No export routing policy is applied to an EVPN instance.

Views

EVPN instance view

Predefined user roles

network-admin

Parameters

route-policy: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify an export routing policy to filter advertised routes or modify their route attributes for EVPN.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply export routing policy **poly-1** to the EVPN instance on VSI **vpna**.

```
<Sysname> system-view
```

```
[Sysname] vsi vpna
```

```
[Sysname-vsi-vpna] evpn encapsulation srv6
```

```
[Sysname-vsi-vpna-evpn-srv6] route-distinguisher 1:1
```

```
[Sysname-vsi-vpna-evpn-srv6] export route-policy poly-1
```

Related commands

route-policy (*Layer 3—IP Routing Command Reference*)

import route-policy

Use **import route-policy** to apply an import routing policy to an EVPN instance.

Use **undo import route-policy** to restore the default.

Syntax

import route-policy *route-policy*
undo import route-policy

Default

No import routing policy is applied to an EVPN instance. The EVPN instance accepts a route when the route targets of the route match local import route targets.

Views

EVPN instance view

Predefined user roles

network-admin

Parameters

route-policy: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify an import routing policy to filter received routes or modify their route attributes for EVPN.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Apply import routing policy **poly-1** to the EVPN instance on VSI **vpna**.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] evpn encapsulation srv6
[Sysname-vsi-vpna-evpn-srv6] route-distinguisher 1:1
[Sysname-vsi-vpna-evpn-srv6] import route-policy poly-1
```

Related commands

route-policy (*Layer 3—IP Routing Command Reference*)

ping evpn vpls srv6

Use **ping evpn vpls srv6** to test the connectivity of an SRv6 PW in an EVPN VPLS over SRv6 network by pinging a remote PE from the local PE.

Syntax

ping evpn vpls srv6 vsi vsi-name mac mac-address [**-a source-ipv6** | **-c count** | **-h hop-limit** | **-m interval** | **-r reply-mode** | **-s packet-size** | **-t time-out** | **-tc tc**] *

Views

Any view

Predefined user roles

network-admin

Parameters

vsi vsi-name: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

mac mac-address: Specifies a host attached to a remote PE by its MAC address in H-H-H format. Do not specify a broadcast MAC address, multicast MAC address, or all-zeros MAC address.

-a source-ipv6: Specifies the source IPv6 address of MPLS echo requests. If you do not specify a source IPv6 address, the IPv6 address of the traffic output interface is used as the source IPv6 address of MPLS echo requests.

-c count: Specifies the number of MPLS echo requests to be sent. The value range for the *count* argument is 1 to 4294967295, and the default value is 5.

-h hop-limit: Specifies the maximum number of hops allowed for an MPLS echo request. The value range for the *hop-limit* argument is 1 to 255, and the default value is 255.

-m interval: Specifies the interval at which an MPLS echo request is sent, in milliseconds. The value range for the *interval* argument is 1 to 10000, and the default value is 2000.

-r reply-mode: Specifies the reply mode used by the receiver (the remote PE) to reply to MPLS echo requests. The value for the *reply-mode* argument can be 2 or 4, and the default value is 2. If the mode is 2, the receiver searches the IP forwarding table for the destination IP address to forward

MPLS echo replies. If the mode is 4, the receiver searches the IPv6 routing table for the source IPv6 address of the echo requests, encapsulates an SRH to the replies, and forwards them.

-s packet-size: Specifies the length of MPLS echo requests, in bytes. The value range for the *packet-size* argument is 81 to 1200, and the default value is 100. The specified packet length does not include the IPv6 header and UDP header length.

-t time-out: Specifies the timeout time of MPLS echo replies, in milliseconds. The value range for the *time-out* argument is 0 to 65535, and the default value is 2000. If the local PE does not receive an MPLS echo reply within the timeout time after sending an MPLS echo request, it determines that the MPLS echo reply times out.

-tc tc: Specifies the traffic class value in MPLS echo requests. The value range for the *tc* argument is 0 to 255 and the default value is 0.

Usage guidelines

In an EVPN VPLS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Use this command to test the connectivity of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs.

Examples

Test the connectivity of the SRv6 PW from the local PE to the remote PE attached to the host with MAC address 2-2-2 in VSI **vpna**.

```
<System> ping evpn vpls srv6 vsi vpna mac 2-2-2
Ping a remote PE in VSI vpna over SRv6 by reaching remote-MAC 0002-0002-0002: 100 data
bytes.
Press CTRL+C to break.
100 bytes from 11::2: sequence=1 time=1 ms
100 bytes from 11::2: sequence=2 time=2 ms
100 bytes from 11::2: sequence=3 time=1 ms
100 bytes from 11::2: sequence=4 time=2 ms
100 bytes from 11::2: sequence=5 time=1 ms

--- Ping statistics for MAC 0002-0002-0002 ---
5 packets transmitted, 5 packets received, 0.0% packets lost
Round-trip min/avg/max = 1/1/2 ms
```

Table 12 Command output

Field	Description
Ping a remote PE in VSI vpna over SRv6 by reaching remote-MAC 0002-0002-0002: 100 data bytes	Ping a remote PE through an SRv6 PW in VSI vpna by reaching remote-MAC 0002-0002-0002. Each MPLS echo request contains 100 bytes.
Press CTRL+C to break	Press escape key Ctrl+C to abort the ping operation.
100 bytes from 11::2: sequence=1 time=1 ms	Received MPLS echo replies from the device whose IPv6 address is 11::2. bytes—Number of bytes in the MPLS echo reply. Sequence—Packet sequence, used to determine whether a segment is lost, disordered or repeated. time—Response time. If no MPLS echo reply is received when the echo reply timeout time expires, the device displays Request time out .
Ping statistics for MAC 0002-0002-0002	Statistics on data received and sent in the ping

Field	Description
	operation.
5 packets transmitted	Number of MPLS echo requests sent.
5 packets received	Number of MPLS echo replies received.
0.0% packets lost	Percentage of unacknowledged packets to the total packets sent.
Round-trip min/avg/max = 1/1/2 ms	Minimum, average, or maximum response time, in milliseconds.

Related commands

tracert evpn vpls srv6

ping evpn vpws srv6

Use **ping evpn vpws srv6** to test the connectivity of an SRv6 PW in an EVPN VPWS over SRv6 network by pinging a remote PE from the local PE.

Syntax

ping evpn vpws srv6 xconnect-group *group-name local-service-id remote-service-id* [**-a** *source-ipv6* | **-c** *count* | **-h** *hop-limit* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-tc** *tc*] *

Views

Any view

Predefined user roles

network-admin

Parameters

xconnect-group *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters. The string cannot contain a hyphen (-).

local-service-id: Specifies a local service ID in the range of 1 to 16777215.

remote-service-id: Specifies a remote service ID in the range of 1 to 16777215.

-a *source-ipv6*: Specifies the source IPv6 address of MPLS echo requests. If you do not specify a source IPv6 address, the IPv6 address of the traffic output interface is used as the source IPv6 address of MPLS echo requests.

-c *count*: Specifies the number of MPLS echo requests to be sent. The value range for the *count* argument is 1 to 4294967295, and the default value is 5.

-h *hop-limit*: Specifies the maximum number of hops allowed for an MPLS echo request. The value range for the *hop-limit* argument is 1 to 255 and the default value is 255.

-m *interval*: Specifies the interval at which an MPLS echo request is sent. The value range for the *interval* argument is 1 to 10000 milliseconds and the default value is 2000 milliseconds.

-r *reply-mode*: Specifies the reply mode used by the receiver (the remote PE) to reply to MPLS echo requests. The value for the *reply-mode* argument can be 2 or 4, and the default value is 2. If the mode is 2, the receiver searches the IP forwarding table for the destination IP address to forward MPLS echo replies. If the mode is 4, the receiver searches the IPv6 routing table for the source IPv6 address of the echo requests, encapsulates an SRH to the replies, and forwards them.

-s packet-size: Specifies the length of MPLS echo requests, in bytes. The value range for the *packet-size* argument is 80 to 1200, and the default value is 100. The specified packet length does not include the IPv6 header and UDP header length.

-t time-out: Specifies the timeout time of MPLS echo replies, in milliseconds. The value range for the *time-out* argument is 0 to 65535, and the default value is 2000. If the local PE does not receive an MPLS echo reply within the timeout time after sending an MPLS echo request, it determines that the MPLS echo reply times out.

-tc tc: Specifies the traffic class value in MPLS echo requests. The value range for the *tc* argument is 0 to 255 and the default value is 0.

Usage guidelines

In an EVPN VPWS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Use this command to test the connectivity of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs.

Examples

Ping a remote PE through an SRv6 PW with local service ID 2 and remote service ID 1 in cross-connect group **xcga**.

```
<Sysname> ping evpn vpws srv6 xconnect-group xcga 2 1
Ping a remote PE over SRv6 through a PW with local service ID 2 and remote service ID 1
in cross-connect group xcga: 100 data bytes.
Press CTRL+C to break.
100 bytes from 111::100: sequence=1 time=2 ms
100 bytes from 111::100: sequence=2 time=2 ms
100 bytes from 111::100: sequence=3 time=1 ms
100 bytes from 111::100: sequence=4 time=1 ms
100 bytes from 111::100: sequence=5 time=2 ms

--- Ping statistics for the PW with local ID 2 and remote ID 1 ---
5 packets transmitted,5 packets received,0.00% packets lost
Round-trip min/avg/max = 1/1/2 ms
```

Table 13 Command output

Field	Description
Ping a remote PE over SRv6 through a PW with local service ID 2 and remote service ID 1 in cross-connect group xcga: 100 data bytes	Ping a remote PE through an SRv6 PW with local service ID 2 and remote service ID 1 in cross-connect group xcga . Each MPLS echo request contains 100 bytes.
Press CTRL+C to break	Press escape key Ctrl+C to abort the ping operation.
100 bytes from 111::100: sequence=5 time=1 ms	Received MPLS echo replies from the device whose IPv6 address is 111::100. bytes—Number of bytes in the MPLS echo reply. sequence—Packet sequence, used to determine whether a segment is lost, disordered or repeated. time—Response time. If no MPLS echo reply is received when the echo reply timeout time expires, the device displays Request time out .
Ping statistics for the PW with local ID 2 and remote ID 1	Statistics on data received and sent in the ping operation.

Field	Description
5 packets transmitted	Number of MPLS echo requests sent.
5 packets received	Number of MPLS echo replies received.
0.0% packets lost	Percentage of unacknowledged packets to the total packets sent.
Round-trip min/avg/max = 1/1/2 ms	Minimum, average, or maximum response time, in milliseconds.

Related commands

tracert evpn vpws srv6

reset l2vpn statistics srv6-pw

Use **reset l2vpn statistics srv6-pw** to clear SRv6 PW packet statistics.

Syntax

```
reset l2vpn statistics srv6-pw [ vsi vsi-name [ peer ipv6-address ] | xconnect-group
group-name [ connection connection-name ] ]
```

Views

User view

Predefined user roles

network-admin

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

peer *ipv6-address*: Specifies a remote PE by its IPv6 address to clear outgoing packet statistics for the SRv6 PWs between the local PE and the specified remote PE. If you do not specify a remote PE, this command clears all SRv6 PW packet statistics for the specified VSI.

xconnect-group *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters.

connection *connection-name*: Specifies a cross-connect by its name, a case-sensitive string of 1 to 20 characters. If you do not specify a cross-connect, this command clears all SRv6 PW packet statistics for the specified cross-connect group.

Usage guidelines

This command clears packet statistics for both primary and backup SRv6 PWs.

If you do not specify any parameters, this command clears all SRv6 PW packet statistics.

Examples

```
# Clear all SRv6 PW packet statistics.
```

```
<Sysname> reset l2vpn statistics srv6-pw
```

Related commands

statistics enable

segment-routing ipv6

Use **segment-routing ipv6** to specify a route recursion mode.

Use **undo segment-routing ipv6** to restore the default.

Syntax

```
segment-routing ipv6 { best-effort | traffic-engineering | traffic-engineering best-effort }
```

```
undo segment-routing ipv6
```

Default

The device searches the IPv6 routing table based on the next hop of a matching EVPN route to forward traffic.

Views

Cross-connect group EVPN instance view

VSI EVPN instance view

Predefined user roles

network-admin

Parameters

best-effort: Specifies the SRv6-BE mode.

traffic-engineering: Specifies the SRv6-TE mode.

traffic-engineering best-effort: Specifies the SRv6-TE and SRv6-BE hybrid mode.

Usage guidelines

Use this command in an EVPN VPWS over SRv6 or EVPN VPLS over SRv6 network.

After the PE receives a customer packet destined for an End.DX2, End.DT2M, or End.DT2U SID, it forwards the packet according to the route recursion mode.

- **SRv6-BE mode**—This mode is also called SID-based forwarding mode. In this mode, the PE first encapsulates the End.DX2, End.DT2M, or End.DT2U SID into the packet. Then, the PE searches the IPv6 routing table based on the SID encapsulated in the packet to forward the packet.
- **SRv6-TE mode**—This mode is also called next hop-based forwarding mode. In this mode, when the PE forwards the packet, it first searches the tunnel policies for a matching SRv6 TE policy based on the next hop of a matching route. Then, the PE adds an SRH to the packet. The SRH includes the End.DX2, End.DT2M, or End.DT2U SID and the SID list of the SRv6 TE policy. Finally, the PE forwards the encapsulated packet through the SRv6 TE policy.
- **SRv6-TE and SRv6-BE hybrid mode**—In this mode, the PE preferentially uses the SRv6-TE mode to forward the packet. If no SRv6 TE policy is available for the packet, the PE forwards the packet in SRv6-BE mode.

Examples

In VSI EVPN instance view, specify the SRv6-BE route recursion mode.

```
<Sysname> system-view
[Sysname] vsi aaa
[Sysname-vsi-aaa] evpn encapsulation srv6
[Sysname-vsi-aaa-mpls-srv6] segment-routing ipv6 best-effort
```

In cross-connect group EVPN instance view, specify the SRv6-BE route recursion mode.

```
<Sysname> system-view
[Sysname] xconnect-group vpna
[Sysname-xcg-vpna] evpn encapsulation srv6
[Sysname-xcg-vpna-evpn-mpls] segment-routing ipv6 best-effort
```

segment-routing ipv6 locator (cross-connect view and VSI EVPN instance view)

Use **segment-routing ipv6 locator** to apply an SRv6 locator to a cross-connect or a VSI.

Use **undo segment-routing ipv6 locator** to remove the specified SRv6 locator from a cross-connect or a VSI.

Syntax

In cross-connect view:

```
segment-routing ipv6 locator locator-name [ dx2l-locator dx2l-locator-name ]  
[ auto-sid-disable ]
```

```
undo segment-routing ipv6 locator
```

In VSI EVPN instance view:

```
segment-routing ipv6 locator locator-name [ dt2u-locator dt2u-locator-name ]  
[ dt2ul-locator dt2ul-locator-name ] [ dx2-locator dx2-locator-name ] [ dx2l-locator  
dx2l-locator-name ] [ auto-sid-disable ]
```

```
undo segment-routing ipv6 locator
```

Default

No SRv6 locators are applied to a cross-connect or a VSI.

Views

Cross-connect view

VSI EVPN instance view

Predefined user roles

network-admin

Parameters

locator-name: Specifies a locator by its name, a case-sensitive string of 1 to 31 characters.

dx2l-locator *dx2l-locator-name*: Specifies the locator used to apply for End.DX2L SIDs. The *dx2l-locator-name* argument represents the locate name, a case-sensitive string of 1 to 31 characters.

dt2u-locator *dt2u-locator-name*: Specifies the locator used to apply for End.DT2U SIDs. The *dt2u-locator-name* argument represents the locate name, a case-sensitive string of 1 to 31 characters.

dt2ul-locator *dt2ul-locator-name*: Specifies the locator used to apply for End.DT2UL SIDs. The *dt2ul-locator-name* argument represents the locate name, a case-sensitive string of 1 to 31 characters.

dx2-locator *dx2-locator-name*: Specifies the locator used to apply for End.DX2 SIDs. The *dx2-locator-name* argument represents the locate name, a case-sensitive string of 1 to 31 characters.

auto-sid-disable: Disables automatic SID allocation. If no opcode is configured for the locator specified in this command when automatic SID allocation is disabled, SID application fails. If you do not specify this keyword, automatic SID allocation is enabled and static SRv6 SIDs and dynamic SRv6 SIDs can coexist. The static SRv6 SIDs take precedence over the dynamically allocated SRv6 SIDs.

Usage guidelines

Use this command to enable a cross-connect or VSI to apply for SRv6 SIDs from the specified locator.

In cross-connect view:

- If you specify the **dx2l-locator** *dx2l-locator-name* option, the *locator-name* argument applies for End.DX2 SIDs and the *dx2l-locator-name* argument applies for End.DX2L SIDs.
- If you do not specify the **dx2l-locator** *dx2l-locator-name* option, the *locator-name* argument applies for both End.DX2 SIDs and End.DX2L SIDs.

In VSI EVPN instance view:

- If you do not specify the **dt2u-locator** *dt2u-locator-name*, **dt2ul-locator** *dt2ul-locator-name*, **dx2-locator** *dx2-locator-name*, or **dx2l-locator** *dx2l-locator-name* option, the *locator-name* argument applies for End.DT2M, End.DT2U, End.DT2UL, End.DX2, and End.DX2L SIDs.
- If you specify the **dt2u-locator** *dt2u-locator-name*, **dt2ul-locator** *dt2ul-locator-name*, **dx2-locator** *dx2-locator-name*, or **dx2l-locator** *dx2l-locator-name* option, the option applies for End.DT2U, End.DT2UL, End.DX2, or End.DX2L SIDs and the *locator-name* argument applies for other SRv6 SIDs.

Examples

Configure VSI **aaa** to use locator **test1** to apply for End.DT2M, End.DT2UL, End.DX2, and End.DX2L SIDs and use locator **test2** to apply for End.DT2U SIDs.

```
<Sysname> system-view
```

```
[Sysname] vsi aaa
```

```
[Sysname-vsi-aaa] evpn encapsulation srv6
```

```
[Sysname-vsi-aaa-evpn-srv6] segment-routing ipv6 locator test1 dt2u-locator test2
```

Configure cross-connect **aaa** in cross-connect group **bbb** to use locator **test3** to apply for End.DX2 and End.DX2L SIDs and disable automatic SID allocation.

```
<Sysname> system-view
```

```
[Sysname] xconnect-group bbb
```

```
[Sysname-xcg-bbb] evpn encapsulation srv6
```

```
[Sysname-xcg-bbb-evpn-srv6] quit
```

```
[Sysname-xcg-bbb] connection aaa
```

```
[Sysname-xcg-bbb-connection-aaa] segment-routing ipv6 locator test3 auto-sid-disable
```

statistics enable

Use **statistics enable** to enable SRv6 PW packet statistics.

Use **undo statistics enable** to disable SRv6 PW packet statistics.

Syntax

statistics enable

undo statistics enable

Default

The SRv6 PW packet statistics feature is disabled.

Views

Cross-connect EVPN PW view

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

EVPN VPWS over SRv6 network:

Use this command to enable SRv6 PW packet statistics in cross-connect EVPN PW view. To display SRv6 PW packet statistics, use the **display l2vpn peer srv6 verbose** command. To clear SRv6 PW packet statistics, use the **reset l2vpn statistics srv6-pw** command.

The **statistics enable** command is not supported by PWs in a cross-connect group EVPN instance that uses MPLS encapsulation.

EVPN VPLS over SRv6 network:

Use the **statistics enable** command to enable packet statistics for all SRv6 PWs in a VSI EVPN instance. To display inbound packet statistics for all SRv6 PWs, use the **display l2vpn statistics srv6-pw inbound** command. To display outbound packet statistics for each SRv6 PW, use the **display l2vpn peer srv6 verbose** command. To clear SRv6 PW packet statistics, use the **reset l2vpn statistics srv6-pw** command.

The **statistics enable** command is supported only by VSI EVPN instances that use SRv6 encapsulation.

Examples

In an EVPN VPWS over SRv6 network, enable packet statistics for an SRv6 PW.

```
<Sysname> system-view
[Sysname] xconnect-group vpws
[Sysname-xcg-vpws] connection aa
[Sysname-xcg-vpws-aa] evpn local-service-id 2 remote-service-id 4
[Sysname-xcg-vpws-aa-2-4] statistics enable
```

In an EVPN VPLS over SRv6 network, enable packet statistics for all SRv6 PWs in an EVPN instance.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] evpn encapsulation srv6
[Sysname-vsi-vpna-evpn-srv6] statistics enable
```

Related commands

display l2vpn peer srv6 verbose

display l2vpn statistics srv6-pw inbound

reset l2vpn statistics srv6-pw

tracert evpn vpls srv6

Use **tracert evpn vpls srv6** to trace the path of an SRv6 PW from the local PE to the remote PE in an EVPN VPLS over SRv6 network.

Syntax

tracert evpn vpls srv6 vsi vsi-name mac mac-address [**-a** source-ipv6 | **-h** hop-limit | **-r** reply-mode | **-t** time-out | **-tc** tc] *

Views

Any view

Predefined user roles

network-admin

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

mac *mac-address*: Specifies a host attached to a remote PE by its MAC address in H-H-H format. Do not specify a broadcast MAC address, multicast MAC address, or all-zeros MAC address.

-a *source-ipv6*: Specifies the source IPv6 address of MPLS echo requests. If you do not specify a source IPv6 address, the IPv6 address of the traffic output interface is used as the source IPv6 address of MPLS echo requests.

-h *hop-limit*: Specifies the maximum number of hops allowed for an MPLS echo request. The value range for the *hop-limit* argument is 1 to 255, and the default value is 255.

-r *reply-mode*: Specifies the reply mode used by the receiver (the remote PE) to reply to MPLS echo requests. The value for the *reply-mode* argument can be 2 or 4, and the default value is 2. If the mode is 2, the receiver searches the IP forwarding table for the destination IP address to forward MPLS echo replies. If the mode is 4, the receiver searches the IPv6 routing table for the source IPv6 address of the echo requests, encapsulates an SRH to the replies, and forwards them.

-t *time-out*: Specifies the timeout time of MPLS echo replies, in milliseconds. The value range for the *time-out* argument is 0 to 65535, and the default value is 2000. If the local PE does not receive an MPLS echo reply within the timeout time after sending an MPLS echo request, it determines that the MPLS echo reply times out.

-tc *tc*: Specifies the traffic class value in MPLS echo replies. The value range for the *tc* argument is 0 to 255 and the default value is 0.

Usage guidelines

In an EVPN VPLS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Use this command to trace the path of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs. This command helps you locate the failed nodes on the path.

Examples

Trace route to a remote PE through an SRv6 PW in VSI **vpna** by reaching remote-MAC 0002-0002-0002.

```
<Sysname> tracert evpn vpls srv6 vsi vpna mac 2-2-2
```

Trace route to a remote PE in VSI vpna over SRv6 by reaching remote-MAC 0002-0002-0002.
Press CTRL+C to break.

Hop	Wait time	Type	Replier
0	0 ms	Ingress	
1	4 ms	Transit	1111::2
2	5 ms	Transit	2222::2
3	6 ms	Transit	3333::2
4	6 ms	Egress	4444::2

Table 14 Command output

Field	Description
Trace route to a remote PE in VSI vpna over SRv6 by reaching remote-MAC 0002-0002-0002	Trace route to a remote PE through an SRv6 PW in VSI vpna by reaching remote-MAC 0002-0002-0002.
Press CTRL+C to break	Press escape key Ctrl+C to abort the tracert operation.
Hop	Hop number.
Wait time	Interval between the time when an echo request was sent and the time when the reply of the echo request was received. The unit is millisecond.

Field	Description
Type	Node type: • Ingress. • Transit. • Egress.
Replier	IPv6 address of the node.
Request time out	This field is available if the local PE does not receive any MPLS echo reply to an MPLS echo request when the echo reply timeout time expires.

Related commands

ping evpn vpls srv6

tracert evpn vpws srv6

Use **tracert evpn vpws srv6** to trace the path of an SRv6 PW from the local PE to the remote PE in an EVPN VPWS over SRv6 network.

Syntax

tracert evpn vpws srv6 xconnect-group *group-name local-service-id remote-service-id* [**-a** *source-ip* | **-h** *hop-limit* | **-r** *reply-mode* | **-t** *time-out* | **-tc** *tc*] *

Views

Any view

Predefined user roles

network-admin

Parameters

xconnect-group *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters. The string cannot contain a hyphen (-).

local-service-id: Specifies a local service ID in the range of 1 to 16777215.

remote-service-id: Specifies a remote service ID in the range of 1 to 16777215.

-a *source-ip*: Specifies the source IPv6 address of MPLS echo requests. If you do not specify a source IPv6 address, the IPv6 address of the traffic output interface is used as the source IPv6 address of MPLS echo requests.

-h *hop-limit*: Specifies the maximum number of hops allowed for an MPLS echo request. The value range for the *hop-limit* argument is 1 to 255, and the default value is 255.

-r *reply-mode*: Specifies the reply mode used by the receiver (the remote PE) to reply to an MPLS echo request. The value for the *reply-mode* argument can be 2 or 4, and the default value is 2. If the mode is 2, the receiver searches the IP forwarding table for the destination IP address to forward MPLS echo replies. If the mode is 4, the receiver searches the IPv6 routing table for the source IPv6 address of the echo requests, encapsulates an SRH to the replies, and forwards them.

-t *time-out*: Specifies the timeout time of MPLS echo replies, in milliseconds. The value range for the *time-out* argument is 0 to 65535, and the default value is 2000. If the local PE does not receive an MPLS echo reply within the timeout time after sending an MPLS echo request, it determines that the MPLS echo reply times out.

-tc *tc*: Specifies the traffic class value in MPLS echo replies. The value range for the *tc* argument is 0 to 255 and the default value is 0.

Usage guidelines

In an EVPN VPWS over SRv6 network, a PE transmits data packets to a remote PE over an SRv6 PW. Use this command to trace the path of the SRv6 PW from the local PE to the remote PE when packet loss or traffic interruption occurs between the PEs. This command helps you locate the failed nodes on the path.

Examples

Trace the route that an SRv6 PW traverses from the local PE to the remote PE in an EVPN VPWS over SRv6 network. The SRv6 PW belongs to cross-connect group **xcga**, its local service ID is 2, and its remote service ID is 1.

```
<Sysname> tracert evpn vpws srv6 xconnect-group xcga 1 2
```

Trace route to a remote PE over SRv6 through a PW with local service ID 2 and remote service ID 1 in cross-connect group xcga.

Press CTRL+C to break.

Hop	Wait time	Type	Replier
0	0 ms	Ingress	
1	4 ms	Transit	1111::2
2	5 ms	Transit	2222::2
3	6 ms	Transit	3333::2
4	6 ms	Egress	3333::2

Table 15 Command output

Field	Description
Trace route to a remote PE over SRv6 through a PW with local service ID 2 and remote service ID 1 in cross-connect group xcga	Trace route to a remote PE through an SRv6 PW with local service ID 2 and remote service ID 1 in cross-connect group xcga .
Hop	Hop number.
Wait time	Interval between the time when an echo request was sent and the time when the reply of the echo request was received. The unit is millisecond.
Press CTRL+C to break	Press escape key Ctrl+C to abort the tracert operation.
Type	Node type: • Ingress. • Transit. • Egress.
Replier	IPv6 address of the node.
Request time out	This field is available if the local PE does not receive any MPLS echo reply to an MPLS echo request when the echo reply timeout time expires.

Related commands

ping evpn vpws srv6

unicast-forwarding dx2-based

Use **unicast-forwarding dx2-based** to configure unicast traffic forwarding based on End.DX2 and End.DX2L SIDs in an EVPN VPLS over SRv6 network.

Use **undo unicast-forwarding dx2-based** to restore the default.

Syntax

unicast-forwarding dx2-based

undo unicast-forwarding dx2-based

Default

Unicast traffic is forwarded based on End.DT2U and End.DT2UL SIDs in an EVPN VPLS over SRv6 network.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

By default, when a PE receives a packet that includes an End.DT2U or End.DT2UL SID, it looks up the MAC address table of the SID's VSI to forward the packet.

To improve forwarding efficiency, use this command. This command enables the PE to allocate an End.DX2 or End.DX2L SID to each AC associated with a VSI and advertise the SIDs to remote PEs through MAC/IP advertisement routes. When the PE receives an SRv6 packet that includes a locally allocated End.DX2 or End.DX2L SID, it does not look up the MAC address table. The PE directly forwards the packet to the AC that is associated with the SID after removing the SRv6 encapsulation.

Examples

Configure EVPN VPLS over SRv6 to forward unicast traffic based on End.DX2 and End.DX2L SIDs.

```
<Sysname> system-view
[Sysname] vsi aaa
[Sysname-vsi-aaa] evpn encapsulation srv6
[Sysname-vsi-aaa-evpn-srv6] unicast-forwarding dx2-based
```

Related commands

segment-routing ipv6 locator (cross-connect view and VSI EVPN instance view)

New feature: Configuring IPv6 Flowspec

Configuring IPv6 Flowspec

Creating and activating an IPv6 Flowspec rule

1. Enter system view.
system-view
2. Create an IPv6 Flowspec rule and enter IPv6 Flowspec rule view.
flow-route flowroute-name ipv6
3. Configure a match criterion.
if-match match-criteria
By default, no match criterion is configured.
4. Configure an action. Choose one option as needed:
 - o Drop packets.

apply deny

- Redirect packets to a next hop.

apply redirect next-hop { *ipv4-address* | *ipv6-address* [**copy-mode**] }

- Redirect packets to an SRv6 TE policy.

apply redirect next-hop *ipv6-address* **color** *color* [**sid** *sid-value*]

- Redirect packets to a route target.

apply redirect vpn-target *import-vpn-target*

- Mark packets with a DSCP value.

apply remark-dscp *dscp-value*

- Rate limit packets.

apply traffic-rate *rate*

By default, no action is configured.

5. (Optional.) Display the match criteria and actions that are not committed.

check flow-route-configuration

6. Commit match criteria and actions.

commit

By default, match criteria and actions are not committed.

Applying an IPv6 Flowspec rule

Applying an IPv6 Flowspec rule to the public network

1. Enter system view.

system-view

2. Enter Flowspec view.

flowspec

3. Create a Flowspec IPv6 address family for the public network and enter its view.

address-family ipv6

4. Apply an IPv6 Flowspec rule to the public network.

flow-route *flowroute-name*

By default, no IPv6 Flowspec rule is applied to the public network.

Applying an IPv6 Flowspec rule to a VPN instance

1. Enter system view.

system-view

2. Configure a VPN instance.

- a. Create a VPN instance and enter VPN instance view.

ip vpn-instance *vpn-instance-name*

- b. Configure an RD for the VPN instance.

route-distinguisher *route-distinguisher*

By default, no RD is configured for a VPN instance.

- c. Configure route targets for the VPN instance.

vpn-target { *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

By default, no route targets are configured.

For more information about the **ip vpn-instance**, **route-distinguisher**, and **vpn-target** commands, see MPLS L3VPN commands in *MPLS Command Reference*.

3. Enter the IPv6 Flowspec address family view of the VPN instance.

address-family ipv6 flowspec

4. Configure route targets for the IPv6 Flowspec address family.

vpn-target *vpn-target*<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

By default, no route targets are configured for the IPv6 Flowspec address family.

The route targets configured must be the same as the route targets configured previously for the VPN instance.

5. Execute the **quit** command twice to return to system view.

6. Enter Flowspec view.

flowspec

7. Create a Flowspec IPv6 address family and associate the address family with the VPN instance.

address-family ipv6 vpn-instance *vpn-instance-name*

8. Apply an IPv6 Flowspec rule to the Flowspec IPv6 VPN instance address family.

flow-route *flowroute-name*

By default, no IPv6 Flowspec rule is applied to a Flowspec IPv6 VPN instance address family.

Enabling BGP to distribute IPv6 Flowspec rules

Restrictions and guidelines

For more information about the **bgp** and **peer enable** commands, see BGP commands in *Layer 3—IP Routing Command Reference*.

Enabling BGP to distribute public network IPv6 Flowspec rules

1. Enter system view.

system-view

2. Execute the following commands in sequence to enter BGP IPv6 Flowspec address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv6 flowspec

3. Enable BGP Flowspec peers to exchange routing information.

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **enable**

By default, BGP Flowspec peers cannot exchange routing information.

4. (Optional.) Disable validation of IPv6 Flowspec rules from BGP Flowspec peers.

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **validation-disable**

By default, IPv6 Flowspec rules from BGP Flowspec peers are validated.

5. (Optional.) Disable validation of the redirection next hops in IPv6 Flowspec rules from BGP Flowspec peers.

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **validation-redirect-disable**

By default, the redirection next hops in IPv6 Flowspec rules from BGP Flowspec peers are validated.

6. (Optional.) Configure the device to not change the next hop of routes advertised to EBGp peers.

```
peer { group-name | | ipv4-address [ mask-length ] ipv6-address [ prefix-length ] }  
next-hop-invariable
```

By default, the device uses its own IP address as the next hop of IPv6 routes advertised to EBGp peers.

7. (Optional.) Enable recursion to tunnels for IPv6 Flowspec rules with an action of redirecting to a next hop.

```
redirect ip recursive-lookup tunnel [ tunnel-selector tunnel-selector-name ]
```

By default, recursion to tunnels is disabled for IPv6 Flowspec rules with an action of redirecting to a next hop.

Enabling BGP to distribute private network IPv6 Flowspec rules

1. Enter system view.

```
system-view
```

2. Execute the following commands in sequence to enter BGP-VPN IPv6 Flowspec address family view:

```
bgp as-number [ instance instance-name ]
```

```
ip vpn-instance vpn-instance-name
```

```
address-family ipv6 flowspec
```

3. Enable BGP Flowspec peers to exchange routing information.

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
enable
```

By default, BGP Flowspec peers cannot exchange routing information.

4. (Optional.) Disable validation of IPv6 Flowspec rules from BGP Flowspec peers.

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
validation-disable
```

By default, IPv6 Flowspec rules from BGP Flowspec peers are validated.

5. (Optional.) Disable validation of the redirection next hops in IPv6 Flowspec rules from BGP Flowspec peers.

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
validation-redirect-disable
```

6. (Optional.) Configure the device to not change the next hop of routes advertised to EBGp peers.

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
next-hop-invariable
```

By default, the device uses its own IP address as the next hop of IPv6 routes advertised to EBGp peers.

Enabling BGP to distribute VPNv6 Flowspec rules

1. Enter system view.

```
system-view
```

2. Execute the following commands in sequence to enter BGP VPNv6 Flowspec address family view:

```
bgp as-number [ instance instance-name ]
```

```
address-family vpnv6 flowspec
```

3. Enable BGP Flowspec peers to exchange routing information.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv4-address* [*mask-length*] }
enable
 By default, BGP Flowspec peers cannot exchange routing information.
4. (Optional.) Configure the device to not change the next hop of VPNv6 routes advertised to EBGp peers.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv4-address* [*mask-length*] }
next-hop-invariable
 By default, the device uses its own IP address as the next hop of VPNv6 routes advertised to EBGp peers.

Configuring BGP Flowspec route reflection

1. Enter system view.
system-view
2. Enter one of the following views:
 - Execute the following commands in sequence to enter BGP IPv6 Flowspec address family view:
bgp as-number [**instance** *instance-name*]
address-family ipv6 flowspec
 - Execute the following commands in sequence to enter BGP-VPN IPv6 Flowspec address family view:
bgp as-number [**instance** *instance-name*]
ip vpn-instance *vpn-instance-name*
address-family ipv6 flowspec
 - Execute the following commands in sequence to enter BGP VPNv6 Flowspec address family view:
bgp as-number [**instance** *instance-name*]
address-family vpnv6 flowspec
3. Configure the router as a route reflector and specify a peer or peer group as its client.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
reflect-client
 By default, no route reflector or client is configured.
4. (Optional.) Disable route target filtering for received BGP VPNv6 Flowspec routes.
undo policy vpn-target
 By default, route target filtering is enabled for received VPNv6 routes. The VPNv6 routes whose export route target attribute matches the local import route target attribute are added to the routing table.
 This command is available only in BGP VPNv6 Flowspec address family view.
5. (Optional.) Enable route reflection between clients.
reflect between-clients
 By default, route reflection between clients is enabled.
6. (Optional.) Configure the cluster ID of the route reflector.
reflector cluster-id { *cluster-id* | *ipv6-address* }
 By default, a route reflector uses its own router ID as the cluster ID.

Disabling the actions in IPv6 Flowspec rules

About this task

If you perform this task, BGP will not notify the QoS module to take the actions in matching IPv6 Flowspec rules.

Restrictions and guidelines

If the **route match-destination** command is executed, BGP uses route prefix 0::0/0 to match the destination address match criterion in the routing policy, and all IPv6 Flowspec rules are matched.

Procedure

1. Enter system view.
system-view
2. Enter one of the following views:
 - Execute the following commands in sequence to enter BGP IPv6 Flowspec address family view:
bgp *as-number* [**instance** *instance-name*]
address-family ipv6 flowspec
 - Execute the following commands in sequence to enter BGP-VPN IPv6 Flowspec address family view:
bgp *as-number* [**instance** *instance-name*]
ip vpn-instance *vpn-instance-name*
address-family ipv6 flowspec
3. Disable the actions in IPv6 Flowspec rules.
routing-table bgp-rib-only [**route-policy** *route-policy-name*]
By default, actions in IPv6 Flowspec rules are executed.

Command reference

New command: address-family ipv6

Use **address-family ipv6** to create a Flowspec IPv6 address family, or enter the view of an existing Flowspec IPv6 address family.

Use **undo address-family ipv6** to delete a Flowspec IPv6 address family and all its settings.

Syntax

address-family ipv6 [**vpn-instance** *vpn-instance-name*]
undo address-family ipv6 [**vpn-instance** *vpn-instance-name*]

Default

No Flowspec IPv6 address family exists.

Views

Flowspec view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Creates the Flowspec IPv6 address family for an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. To create a Flowspec IPv6 address family for the public network, do not specify this option.

Examples

Create a Flowspec IPv6 address family for the public network and enter its view.

```
<Sysname> system-view
[Sysname] flowspec
[Sysname-flowspec] address-family ipv6
[Sysname-flowspec-ipv6]
```

New command: address-family ipv6 flowspec (BGP instance view)

Use **address-family ipv6 flowspec** to create a BGP IPv6 Flowspec address family, or enter the view of an existing BGP IPv6 Flowspec address family.

Use **undo address-family ipv6 flowspec** to delete a BGP IPv6 Flowspec address family and all its settings.

Syntax

address-family ipv6 flowspec
undo address-family ipv6 flowspec

Default

No BGP IPv6 Flowspec address family exists.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

The settings in the view of a BGP IPv6 Flowspec address family take effect only on routes and peers of the BGP IPv6 Flowspec address family.

Examples

Create a BGP IPv6 Flowspec address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv6 flowspec
[Sysname-bgp-default-ipv6-flowspec]
```

New command: address-family ipv6 flowspec (BGP-VPN instance view)

Use **address-family ipv6 flowspec** to create a BGP-VPN IPv6 Flowspec address family, or enter the view of an existing BGP-VPN IPv6 Flowspec address family.

Use **undo address-family ipv6 flowspec** to delete a BGP-VPN IPv6 Flowspec address family and all its settings.

Syntax

address-family ipv6 flowspec
undo address-family ipv6 flowspec

Default

No BGP-VPN IPv6 Flowspec address family exists.

Views

BGP-VPN instance view

Predefined user roles

network-admin

Usage guidelines

The settings in the view of a BGP-VPN IPv6 Flowspec address family take effect only on routes and peers of the BGP-VPN IPv6 Flowspec address family.

Examples

Create a BGP-VPN IPv6 Flowspec address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] ip vpn-instance vpn1
[Sysname-bgp-default-vpn1] address-family ipv6 flowspec
[Sysname-bgp-default-flowspec-ipv6-vpn1]
```

Related commands

bgp (*Layer 3—IP Routing Command Reference*)

ip vpn-instance (*MPLS Command Reference*)

New command: address-family vpnv6 flowspec

Use **address-family vpnv6 flowspec** to create a BGP VPNv6 Flowspec address family, or enter the view of an existing BGP VPNv6 Flowspec address family.

Use **undo address-family vpnv6 flowspec** to delete a BGP VPNv6 Flowspec address family and all its settings.

Syntax

address-family vpnv6 flowspec
undo address-family vpnv6 flowspec

Default

No BGP VPNv6 Flowspec address family exists.

Views

BGP instance view

Predefined user roles

network-admin

Examples

Create a BGP VPNv6 Flowspec address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family vpnv6 flowspec
[Sysname-bgp-default-vpnv6-flowspec]
```

Related commands

bgp (Layer 3—IP Routing Command Reference)

Modified command: apply

Syntax

apply *action*

undo apply *action*

Old views

IPv4 Flowspec rule view

New views

IPv4 Flowspec rule view

IPv6 Flowspec rule view

Change description

The IPv6 Flowspec rule view is added, and the following redirection actions are added:

Table 16 Redirection actions

Action	Description
redirect next-hop { <i>ipv4-address</i> <i>ipv6-address</i> } [copy-mode]	Redirects packets to a next hop: • <i>ipv4-address</i>: Specifies the IPv4 address of the next hop. • <i>ipv6-address</i>: Specifies the IPv6 address of the next hop. • copy-mode: Redirects copies of the packets.
redirect next-hop <i>ipv6-address</i> color <i>color</i> [sid <i>sid-value</i>]	Redirects packets to an SRv6 TE policy: • <i>ipv6-address</i>: Specifies the destination node address of the SRv6 TE policy. • color <i>color</i>: Specifies the color attribute of the SRv6 TE policy:, in the format of <i>CO (color-only) flag:color attribute value</i>. The range value for the CO flag is 00 to 11. • sid <i>sid-value</i>: Specifies the SRv6 SID of the egress node. The device adds the SRv6 SID to the SRH header and places it after the SID list. After the packets are forwarded to the egress node, the egress node takes the forwarding action based on the SRv6 SID. For more information about SRv6 TE policies, see <i>Segment Routing Configuration Guide</i> .
redirect vpn-target <i>import-vpn-target</i>	Redirects packets to a route target. The <i>import-vpn-target</i> argument specifies a route target, a string of 3 to 21 characters. A route target can be indicated in one of the following formats: • 16-bit AS number:32-bit user-defined number, for example, 100:3. • 32-bit IP address:16-bit user-defined number, for example, 192.168.122.15:1. • 32-bit AS number:16-bit user-defined number, for example, 65536:1. The

Action	Description
	smallest AS number is 65536.

Modified command: check flow-route-configuration

Old views

IPv4 Flowspec rule view

New views

IPv4 Flowspec rule view

IPv6 Flowspec rule view

Change description

The IPv6 Flowspec rule view is added.

Modified command: commit

Old views

IPv4 Flowspec rule view

New views

IPv4 Flowspec rule view

IPv6 Flowspec rule view

Change description

The IPv6 Flowspec rule view is added.

New command: display bgp group flowspec

Use **display bgp group flowspec** to display BGP peer group information.

Syntax

```
display bgp [ instance instance-name ] group { ipv4 | ipv6 | vpnv4 | vpnv6 } flowspec
[ vpn-instance vpn-instance-name ] [ group-name group-name ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays the information for the default BGP instance.

ipv4: Displays IPv4 BGP peer group information.

ipv6: Displays IPv6 BGP peer group information.

vpnv4: Displays VPNv4 BGP peer group information.

vpn6: Displays VPNv6 BGP peer group information.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the information for the public network.

group-name *group-name*: Specifies a BGP peer group by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a group, this command displays brief information about all BGP peer groups for the specified address family.

Examples

Display brief information about all BGP IPv4 peer groups.

```
<Sysname> display bgp group ipv4 flowspec
```

```
BGP peer group: group1
```

```
Remote AS: 600
```

```
Authentication type configured: None
```

```
Type: external
```

```
Members:
```

```
1.1.1.10
```

```
BGP peer group: group2
```

```
Remote AS number: not specified
```

```
Type: external
```

```
Members:
```

```
2.2.2.2
```

Table 17 Command output

Field	Description
BGP peer group	Name of the BGP peer group.
Remote AS	AS number of the peer group.
Authentication type configured	Authentication mode of the peer group: • None. • MD5. • Keychain (<i>keychain-name</i>).
Type	Type of the peer group: • external—EBGP peer group. • internal—IBGP peer group.
Maximum number of prefixes allowed	Maximum number of routes allowed to learn from the peer. This field does not apply to BGP L2VPN.
Threshold	Percentage of received routes from the peer to maximum routes allowed to learn from the peer. If the percentage is reached, the system generates a log message. This field does not apply to BGP L2VPN.
Configured hold time	Configured hold interval in seconds.
Keepalive time	Keepalive interval in seconds.
Minimum time between advertisements	Minimum route advertisement interval in seconds.
Peer preferred value	Preferred value specified for routes from the peer. This field does not apply to BGP L2VPN.

Field	Description
Site-of-Origin	SoO for the peer group.
Routing policy configured	Routing policy configured for the peer group. If you do not specify a routing policy, this field displays No routing policy is configured . This field does not apply to BGP L2VPN.
Members	Information about peers included in the peer group.
* - Dynamically created peer	An asterisk (*) before a peer address indicates that the peer is a dynamic peer.
Peer	IPv4 or IPv6 address of the peer.
AS	AS number of the peer.
MsgRcvd	Number of messages received.
MsgSent	Number of messages sent.
OutQ	Number of messages to be sent.
PrefRcv	For the IPv4, IPv6, VPNv4, and VPNv6 address families, this field displays the number of prefixes received from the peer. For MPLS L2VPN, this field displays the number of label blocks received from the peer. For VPLS, this field displays the total number of label blocks and VPLS PEs discovered by BGP. For the IPv4 flowspec address family, this field displays the number of IPv4 flowspec messages received from the peer. For the IPv4 MDT address family, this field displays the number of MDT messages received from the peer.
Up/Down	Lasting time of the current BGP session state.
State	Current state of the BGP session between the local router and the peer.
IPsec profile name	IPsec profile applied to the IPv6 BGP peer group.

New command: display bgp routing-table ipv6 flowspec

Use **display bgp routing-table ipv6 flowspec** to display BGP IPv6 Flowspec routing information.

Syntax

```
display bgp [ instance instance-name ] routing-table ipv6 flowspec [ vpn-instance vpn-instance-name ] [ flowspec-prefix [ advertise-info ] | statistics ]
```

```
display bgp [ instance instance-name ] routing-table ipv6 flowspec [ vpn-instance vpn-instance-name ] peer { ipv4-address | ipv6-address } { advertised-routes | received-routes } [ flowspec-prefix | statistics ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays the information for the default BGP instance.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays the information for the public network.

flowspec-prefix: Displays detailed BGP IPv6 Flowspec routing information. The values for this argument are the values under the **Network** field displayed when you do not specify this argument.

advertise-info: Displays advertisement information for BGP IPv6 Flowspec routes.

peer { *ipv4-address* | *ipv6-address* }: Displays BGP IPv4 or IPv6 Flowspec routing information advertised to or received from the specified peer.

advertised-routes: Displays BGP IPv6 Flowspec routing information advertised to the specified peer.

received-routes: Displays BGP IPv6 Flowspec routing information received from the specified peer.

statistics: Displays routing statistics.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP IPv6 Flowspec routes.

Examples

Display brief information about all public-network BGP IPv6 Flowspec routes in the default BGP instance.

```
<Sysname> display bgp routing-table ipv6 flowspec
```

```
Total number of routes: 1
```

```
BGP local router ID is 10::1
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
              s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >e DEST:11::1/64,Proto:=0 1 =60,DPort:=200,SPort:=100,ICMPType:=200/176	0.0.0.0			0	200?

Display information about public-network BGP IPv6 Flowspec routes advertised to peer 10::1 in the default BGP instance.

```
<Sysname> display bgp routing-table ipv6 flowspec peer 10::1 advertised-routes
```

```
Total number of routes: 1
```

```
BGP local router ID is 10::2
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
              s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

```

Network          NextHop          MED          LocPrf          Path/Ogn

* >  DEST:11::1/64,Proto:=0|1|=60,DPort:=200,SPort:=100,ICMPType:=200/176
                                0.0.0.0                                200?

# Display information about public-network BGP IPv6 Flowspec routes received from peer 10::2 in
the default BGP instance.

<Sysname> display bgp routing-table ipv6 flowspec peer 10::2 received-routes

Total number of routes: 1

BGP local router ID is 10::1
Status codes: * - valid, > - best, d - dampened, h - history,
              s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete

Network          NextHop          MED          LocPrf          PrefVal Path/Ogn

* >e  DEST:11::1/64,Proto:=0|1|=60,DPort:=200,SPort:=100,ICMPType:=200/176
                                0.0.0.0                                0          200?

```

Table 18 Command output

Field	Description
Status codes	Status codes: • * – valid—Valid route. • > – best—Optimal route. • d – dampened—Dampened route. • h – history—History route. • s – suppressed—Suppressed route. • S – stale—Stale route. • i – internal—Internal route. • e – external—External route.
Origin	Origin of the route: • i – IGP—Originated in the AS. The origin of routes advertised with the network command is IGP. • e – EGP—Learned through EGP. • ? – incomplete—Unknown origin. The origin of routes redistributed from IGP protocols is incomplete.
Network	Destination network address.
NextHop	Next-hop IP address.
MED	Multi-Exit Discriminator attribute.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • AS_PATH—Records the ASs the route has passed. This attribute can avoid routing loops. • ORIGIN—Identifies the origin of the route.

Display statistics for BGP IPv6 Flowspec routes advertised to peer 10::2 in the default BGP instance.

```
<Sysname> display bgp routing-table ipv6 flowspec peer 10::2 advertised-routes statistics
```

```
Advertised routes total: 2
```

Display statistics for BGP IPv6 Flowspec routes received from peer 10::2 in the default BGP instance.

```
<Sysname> display bgp routing-table ipv6 flowspec peer 10::2 received-routes statistics
```

```
Received routes total: 2
```

Table 19 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display information about public-network BGP IPv6 Flowspec routes to destination network with DPort as 1000/32 in the default BGP instance.

```
<Sysname> display bgp routing-table ipv6 flowspec DPort:=1000/32
```

```
BGP local router ID: 1.1.1.2
```

```
Local AS number: 100
```

```
Paths: 1 available, 1 best
```

```
BGP routing table information of DPort:=1000/32:
```

```
Imported route.
```

```
Original nexthop: 0.0.0.0
```

```
Out interface : NULL0
```

```
Route age : 00h00m10s
```

```
OutLabel : NULL
```

```
Ext-Community : <CO-Flag:Color(00:1)>
```

```
Ext-Community6 : <FLOWSPEC REDIRECT-IP: 11::1:0>
```

```
RxPathID : 0x0
```

```
TxPathID : 0x0
```

```
Org-validation : Valid
```

```
PrefixSID : N/A SID <123::1>
```

```
AS-path : (null)
```

```
Origin : igp
```

```
Attribute value : pref-val 32768
```

```
State : valid, local, best
```

```
IP precedence : N/A
```

```
QoS local ID : N/A
```

```
Traffic index : N/A
```

Table 20 Command output

Field	Description
Paths	Number of routes:

Field	Description
	• available—Number of valid routes. • best—Number of optimal routes.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP UPDATE message, the original next hop is the next hop IP address in the message.
Out interface	Next hop output interface information.
Route age	Time elapsed since the most recent route update.
OutLabel	Outgoing label of the route.
Ext-Community	Extended community attribute.
Ext-Community6	IPv6 extended community attribute.
RxPathID	Add-path ID of received routes.
TxPathID	Add-path ID of advertised routes.
Org-validation	BGP RPKI validation state: • Valid. • Not found. • Invalid.
PrefixSID	Prefix SID: • Label index—Label index. • SRGB—SRGB range.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: • igp—Originated in the AS. • egp—Learned through EGP. • incomplete—Unknown origin.
Attribute value	BGP path attributes: • MED—MED value. • localpref—Local preference value. • pref-val—Preferred value. • pre—Route preference.
State	Current state of the route: • valid. • internal. • external. • local. • synchronize. • best. • delay—The route will be delayed for optimal route selection. This field is displayed only in the detailed command output. • bgp-rib-only—The route will not be flushed to the routing table. This field is displayed only in the detailed command output. • not preferred for reason—Reason why the route is not selected as the optimal route. • not ECMP for reason—Reason why the route does not form ECMP routes with other routes.
IP precedence	IP precedence in the range of 0 to 7. N/A indicates that the route does

Field	Description
	not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. N/A indicates that the route does not support this field.
Traffic index	Traffic index in the range of 1 to 64. N/A indicates that the route does not support this field.

New command: display bgp routing-table vpnv6 flowspec

Use **display bgp routing-table vpnv6 flowspec** to display BGP VPNv6 Flowspec routing information.

Syntax

```
display bgp [ instance instance-name ] routing-table vpnv6 flowspec [ peer
{ ipv4-address | ipv6-address } { advertised-routes | received-routes } [ flowspec-prefix
| statistics ] ] [ route-distinguisher route-distinguisher ] [ flowspec-prefix
[ advertise-info ] ] | statistics ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays the information for the default BGP instance.

peer { *ipv4-address* | *ipv6-address* }: Displays BGP VPNv4 or VPNv6 Flowspec routing information advertised to or received from the specified peer.

advertised-routes: Displays BGP VPNv6 Flowspec routing information advertised to the specified peer.

received-routes: Displays BGP VPNv6 Flowspec routing information received from the specified peer.

route-distinguisher *route-distinguisher*: Displays BGP VPNv6 Flowspec routing information for the specified route distinguisher. The *route-distinguisher* argument is a string of 3 to 21 characters and can be specified in one of the following formats:

- 16-bit AS number:32-bit user-defined number, for example, 101:3.
- 32-bit IP address:16-bit user-defined number, for example, 192.168.122.15:1.
- 32-bit AS number:16-bit user-defined number, for example, 65536:1. The smallest AS number is 65535.

flowspec-prefix: Displays detailed BGP VPNv6 Flowspec routing information. The values for this argument are the values under the **Network** field displayed when you do not specify this argument.

advertise-info: Displays advertisement information for BGP VPNv6 Flowspec routes.

statistics: Displays routing statistics.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP VPNv6 Flowspec routes.

Examples

Display brief information about all BGP VPNv6 Flowspec routes in the default BGP instance.

```
<Sysname> display bgp routing-table vpnv6 flowspec
```

```
BGP local router ID is 1::1
```

```
Status codes: * - valid, > - best, d - dampened, h - history,
               s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

```
Total number of routes from all PEs: 4
```

```
Route distinguisher: 1:3
```

```
Total number of routes: 2
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >i DEST:2::1/32,Source:3::1/32,Proto:=0 =1 =60,Port:=200,DPort:=200 =300 ,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFl ags:=255,Length:=1024,DSCP:=6 =2,Frag:=4/528					
	0.0.0.0		100	0	?
* >i DEST:4::1/32,Proto:=0 =1 =60,DPort:=200,SPort:=100,ICMPType:=200/176					
	0.0.0.0		100	0	?

```
Route distinguisher: 1:5(vpn1)
```

```
Total number of routes: 5
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >i DEST:2::1/32,Source:3::1/32,Proto:=0 =1 =60,Port:=200,DPort:=200 =300 ,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFl ags:=255,Length:=1024,DSCP:=6 =2,Frag:=4/528					
	0.0.0.0		100	0	?
* >e DEST:4::1/32,Source:3::1/32,Proto:=0 =1 =60,Port:=200,DPort:=200 =300 ,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFl ags:=255,Length:=1024,DSCP:=6 =2,Frag:=4,DEST:2::1/32,Source:3::1/32,Proto :=0 =1 =60,Port:=200,DPort:=200 =300,SPort:=100 =120 =140,ICMPType:=200 =100 =12 0 =140,ICMPCode:=200 =220 =230,TCPFlags:=255,Length:=1024,DSCP:=6 =2,Frag:=4/1056					
	0.0.0.0			0	100?
* > DEST:4::1/32,Proto:=0 =1 =60,DPort:=200,SPort:=100,ICMPType:=200/176					
	0.0.0.0			32768	?
* i	0.0.0.0		100	0	?
* e	0.0.0.0			0	100?

```
Route distinguisher: 1:6
```

```
Total number of routes: 2
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >e DEST:2::1/32,Source:3::1/32,Proto:=0 1 =60,Port:=200,DPort:=200 =300,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFlags:=255,Length:=1024,DSCP:=6 =2,Frag:=4,DEST:2::1/32,Source:3::1/32,Proto:=0 1 =60,Port:=200,DPort:=200 =300,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFlags:=255,Length:=1024,DSCP:=6 =2,Frag:=4/1056					
	0.0.0.0			0	100?
* >e DEST:4::1 /32,Proto:=0 1 =60,DPort:=200,SPort:=100,ICMPType:=200/176					
	0.0.0.0			0	100?

Display brief information about all BGP VPNv6 Flowspec routes with route distinguisher 1:5 in the default BGP instance.

```
<Sysname> display bgp routing-table vpnv6 flowspec route-distinguisher 1:5
```

```
BGP local router ID is 192.168.56.55
Status codes: * - valid, > - best, d - dampened, h - history,
              s - suppressed, S - stale, i - internal, e - external
Origin: i - IGP, e - EGP, ? - incomplete
```

```
Route distinguisher: 1:5(vpn1)
Total number of routes: 5
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >i DEST:2::1/32,Source:3::1/32,Proto:=0 1 =60,Port:=200,DPort:=200 =300,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFlags:=255,Length:=1024,DSCP:=6 =2,Frag:=4/528					
	0.0.0.0		100	0	?
* >e DEST:2::1/32,Source:3::1/32,Proto:=0 1 =60,Port:=200,DPort:=200 =300,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFlags:=255,Length:=1024,DSCP:=6 =2,Frag:=4,DEST:2::1/32,Source:3::1/32,Proto:=0 1 =60,Port:=200,DPort:=200 =300,SPort:=100 =120 =140,ICMPType:=200 =100 =120 =140,ICMPCode:=200 =220 =230,TCPFlags:=255,Length:=1024,DSCP:=6 =2,Frag:=4/1056					
	0.0.0.0			0	100?
* > DEST:4::1/32,Proto:=0 1 =60,DPort:=200,SPort:=100,ICMPType:=200/176					
	0.0.0.0			32768	?
* i	0.0.0.0		100	0	?
* e	0.0.0.0			0	100?

Table 21 Command output

Field	Description
Status codes	Status codes: • * – valid—Valid route. • > – best—Optimal route. • d – dampened—Dampened route. • h – history—History route. • i – internal—Internal route. • e – external—External route. • s – suppressed—Suppressed route. • S – stale—Stale route.
Origin	Origin of the route: • i – IGP—Originated in the AS. The origin of routes advertised with the network command is IGP. • e – EGP—Learned through EGP. • ? – incomplete—Unknown origin. The origin of routes redistributed from IGP protocols is incomplete.
Network	Destination network address.
NextHop	Next hop IP address.
MED	Multi-Exit Discriminator attribute.
LocPrf	Local preference value.
PrefVal	Preferred value of the route.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • AS_PATH—Records the ASs the route has passed. This attribute can avoid routing loops. • ORIGIN—Identifies the origin of the route.

Display statistics for BGP VPNv6 Flowspec routes advertised to peer 15.5.6.2 in the default BGP instance.

```
<Sysname> display bgp routing-table vpnv6 flowspec peer 15.5.6.2 advertised-routes statistics
```

```
Advertised routes total: 3
```

Display statistics for BGP VPNv6 Flowspec routes received from peer 15.5.6.2 in the default BGP instance.

```
<Sysname> display bgp routing-table vpnv6 flowspec peer 15.5.6.2 received-routes statistics
```

```
Received routes total: 2
```

Table 22 Command output

Field	Description
Advertised routes total	Total number of advertised routes.
Received routes total	Total number of received routes.

Display statistics for BGP VPNv6 Flowspec routes.

```
<Sysname> display bgp routing-table vpnv6 flowspec statistics
```

Total number of routes from all PEs: 4

Route distinguisher: 1:3

Total number of routes: 2

Route distinguisher: 1:5(vpn1)

Total number of routes: 5

Route distinguisher: 1:6

Total number of routes: 2

Display information about public-network BGP VPNv6 Flowspec routes to destination network with DPort as 1000/32 in the default BGP instance.

<Sysname> display bgp routing-table vpnv6 flowspec DPort:=1000/32

BGP local router ID: 192.168.56.11

Local AS number: 1

Route distinguisher: 1:1(1)

Total number of routes: 1

Paths: 1 available, 1 best

BGP routing table information of DPort:=1000/32:

Imported route.

Original nexthop: 0.0.0.0

Out interface : NULL0

Route age : 00h00m26s

OutLabel : NULL

Ext-Community : <RT: 1:1>, <CO-Flag:Color(00:1)>

Ext-Community6 : <FLOWSPEC REDIRECT-IP: 1::1:0>

RxPathID : 0x0

TxPathID : 0x0

Org-validation : Valid

PrefixSID : N/A SID <111::1>

AS-path : (null)

Origin : igp

Attribute value : pref-val 32768

State : valid, local, best

IP precedence : N/A

QoS local ID : N/A

Traffic index : N/A

Table 23 Command output

Field	Description
Paths	Number of routes: • available—Number of valid routes. • best—Number of optimal routes.
Original nexthop	Original next hop of the route. If the route was obtained from a BGP

Field	Description
	UPDATE message, the original next hop is the next hop IP address in the message.
Out interface	Next hop output interface information.
Route age	Time elapsed since the most recent route update.
OutLabel	Outgoing label of the route.
Ext-Community	Extended community attribute.
Ext-Community6	IPv6 extended community attribute.
RxPathID	Add-path ID of received routes.
TxPathID	Add-path ID of advertised routes.
Org-validation	BGP RPKI validation state: - Valid. - Not found. - Invalid.
PrefixSID	Prefix SID: Label index—Label index. SRGB—SRGB range.
AS-path	AS_PATH attribute of the route, which records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: igp—Originated in the AS. egp—Learned through EGP. incomplete—Unknown origin.
Attribute value	BGP path attributes: MED—MED value. localpref—Local preference value. pref-val—Preferred value. pre—Route preference.
State	Current state of the route: valid. internal. external. local. synchronize. best. delay—The route will be delayed for optimal route selection. This field is displayed only in the detailed command output. bgp-rib-only—The route will not be flushed to the routing table. This field is displayed only in the detailed command output. not preferred for reason—Reason why the route is not selected as the optimal route. not ECMP for reason—Reason why the route does not form ECMP routes with other routes.
IP precedence	IP precedence in the range of 0 to 7. N/A indicates that the route does not support this field.
QoS local ID	QoS local ID in the range of 1 to 4095. N/A indicates that the route does not support this field.

Field	Description
Traffic index	Traffic index in the range of 1 to 64. N/A indicates that the route does not support this field.

Modified command: display flow-route

Old syntax

In standalone mode:

display flow-route { **all** | *flow-route-id* | **ip** [**vpn-instance** *vpn-instance-name*] }

In IRF mode:

display flow-route { **all** | *flow-route-id* | **ip** [**vpn-instance** *vpn-instance-name*] } [**slot** *slot-number*]

New syntax

In standalone mode:

display flow-route { **all** | { **ip** | **ipv6** } [**all** | **vpn-instance** *vpn-instance-name*] | *flow-route-id* }

In IRF mode:

display flow-route { **all** | { **ip** | **ipv6** } [**all** | **vpn-instance** *vpn-instance-name*] | *flow-route-id* } [**slot** *slot-number*]

Views

Any view

Change description

The following parameter is added:

ipv6: Specifies IPv6 Flowspec rules.

Modified command: flow-route (Flowspec IPv4 address family view)

Syntax

flow-route *flowroute-name*

undo flow-route *flowroute-name*

Old views

IPv4 Flowspec rule view

New views

IPv4 Flowspec rule view

IPv6 Flowspec rule view

Change description

The IPv6 Flowspec rule view is added.

New command: flow-route ipv6 (system view)

Use **flow-route ipv6** to create an IPv6 Flowspec rule, or enter the view of an existing IPv6 Flowspec rule.

Use **undo flow-route ipv6** to delete an IPv6 Flowspec rule.

Syntax

flow-route *flowroute-name* **ipv6**

undo flow-route *flowroute-name* **ipv6**

Default

Non IPv6 Flowspec rules exist.

Views

System view

Predefined user roles

network-admin

Parameters

flowroute-name: Specifies an IPv6 Flowspec rule name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete an IPv6 Flowspec rule applied to a Flowspec IPv6 address family, perform the following tasks:

1. Execute the **undo flow-route ipv6** command in Flowspec IPv6 address family view.
2. Execute the **undo flow-route ipv6** command in system view.

Examples

Create an IPv6 Flowspec rule named **route1**.

```
<Sysname> system-view
[Sysname] flow-route route1 ipv6
[Sysname-flow-route-ipv6-route1]
```

Modified command: if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Old views

IPv4 Flowspec rule view

New views

IPv4 Flowspec rule view

IPv6 Flowspec rule view

Change description

The IPv6 Flowspec rule view is added, and the following match criteria are added:

Table 24 Added match criteria

Match criterion type ID	Option	Description
1	destination-ipv6 { <i>ipv6-address</i> <i>prefix-length</i> <i>ipv6-address/prefix-length</i> }	Matches the destination IPv6 address of packets. The <i>ipv6-address</i> argument specifies an IPv6 address in sets of 16-bit hexadecimal values separated by colons (:). The <i>prefix-length</i> argument specifies the prefix length in the range of 0 to 128.
2	source-ipv6 { <i>ipv6-address</i> <i>prefix-length</i> <i>ipv6-address/prefix-length</i> }	Matches the source IPv6 address of packets. The <i>ipv6-address</i> argument specifies an IPv6 address in sets of 16-bit hexadecimal values separated by colons (:). The <i>prefix-length</i> argument specifies the prefix length in the range of 0 to 128.
3	next-header { <i>next-header-list</i> <i>next-header-name</i> &<1-8> }	Matches the protocol in an IPv6 next header. The <i>next-header-list</i> argument specifies a space-separated list of up to eight protocol items. Each item specifies a protocol or a range of protocols by numerical values in the form of <i>next-header-start to next-header-end</i> . The value for <i>next-header-end</i> must be greater than or equal to the value for <i>next-header-start</i> . The value range for the <i>next-header</i> argument is 0 to 255. The <i>next-header-name</i> argument specifies up to eight protocols by keyword. The available keywords are: icmp (1), igmp (2), ipinip (4), tcp (6), egp (8), udp (17), ipv6 (41), rsvp (46), gre (47), esp (50), icmpv6 (58), ospf (89), and pim (103).
13	flow-label <i>flow-label-list</i>	Matches the IPv6 flow label. The <i>flow-label-list</i> argument specifies a space-separated list of up to eight flow label items. Each item specifies a protocol or a range of protocols by numerical values in the form of <i>flow-label-start to flow-label-end</i> . The value for <i>flow-label-end</i> must be greater than or equal to the value for <i>flow-label-start</i> . The value range for the <i>flow-label</i> argument is 0 to 1048575.

Modified command: peer next-hop-invariable

Old syntax

peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-invariable**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-invariable**

New syntax

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
next-hop-invariable  
  
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
next-hop-invariable
```

Old views

BGP IPv4 Flowspec address family view
BGP-VPN IPv4 Flowspec address family view
BGP VPNv4 Flowspec address family view

New views

BGP IPv4 Flowspec address family view
BGP-VPN IPv4 Flowspec address family view
BGP VPNv4 Flowspec address family view
BGP IPv6 Flowspec address family view
BGP-VPN IPv6 Flowspec address family view
BGP VPNv6 Flowspec address family view

Change description

The BGP IPv6 Flowspec address family view, BGP-VPN IPv6 Flowspec address family view, and BGP VPNv6 Flowspec address family view are added, and the following parameters are added:

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, the device does not change the next hop of routes advertised to all dynamic peers in the subnet.

New command: peer redirect ip rfc-compatible

Use **peer redirect ip rfc-compatible** to configure the attribute ID for the redirection next hop in IPv4 Flowspec rules as the RFC-specified 0x010C.

Use **undo peer redirect ip rfc-compatible** to restore the default.

Syntax

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
redirect ip rfc-compatible  
  
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
redirect ip rfc-compatible
```

Default

The attribute ID for the redirection next hop in static IPv4 Flowspec rules is 0x0800, and the attribute ID for the redirection next hop in dynamic IPv4 Flowspec rules is received from the peer.

Views

BGP IPv4 Flowspec address family view
BGP-VPN IPv4 Flowspec address family view
BGP-VPNv4 Flowspec address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters.

ipv4-address: Specifies a peer by its IPv4 address.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a mask length, all dynamic peers in the subnet are specified.

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a prefix length in this command, all dynamic peers in the subnet are specified.

Usage guidelines

Two attribute IDs for the redirection next hop exist: RFC-specified 0x010C and IETF-specified 0x0800. To interoperate with a third-party device that does not support IETF-specified 0x0800, you can use execute this command.

Examples

Configure the attribute ID for the redirection next hop in IPv4 Flowspec rules as the RFC-specified 0x010C.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 flowspec
[Sysname-bgp-default-flowspec-ipv4] peer 1.1.1.1 redirect ip rfc-compatible
```

Modified command: peer reflect-client

Old syntax

peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

New syntax

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **reflect-client**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **reflect-client**

Old views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP VPNv4 Flowspec address family view

New views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP VPNv4 Flowspec address family view

BGP IPv6 Flowspec address family view

BGP-VPN IPv6 Flowspec address family view

BGP VPNv6 Flowspec address family view

Change description

The BGP IPv6 Flowspec address family view, BGP-VPN IPv6 Flowspec address family view, and BGP VPNv6 Flowspec address family view are added, and the following parameters are added:

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, the device does not change the next hop of routes advertised to all dynamic peers in the subnet.

Modified command: peer validation-disable

Old syntax

peer { *group-name* | *ip-address* [*mask-length*] } **validation-disable**

undo peer { *group-name* | *ip-address* [*mask-length*] } **validation-disable**

New syntax

peer { *group-name* | *ip-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **validation-disable**

undo peer { *group-name* | *ip-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **validation-disable**

Old views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

New views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP IPv6 Flowspec address family view

BGP-VPN IPv6 Flowspec address family view

Change description

The BGP IPv6 Flowspec address family view and BGP-VPN IPv6 Flowspec address family view are added, and the following parameters are added:

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, the device does not change the next hop of routes advertised to all dynamic peers in the subnet.

Modified command: peer validation-redirect-disable

Old syntax

peer { *group-name* | *ip-address* [*mask-length*] } **validation-redirect-disable**

undo peer { *group-name* | *ip-address* [*mask-length*] } **validation-redirect-disable**

New syntax

```
peer { group-name | ip-address [ mask-length ] | ipv6-address [ prefix-length ] }  
validation-redirect-disable  
  
undo peer { group-name | ip-address [ mask-length ] | ipv6-address [ prefix-length ] }  
validation-redirect-disable
```

Old views

BGP IPv4 Flowspec address family view
BGP-VPN IPv4 Flowspec address family view

New views

BGP IPv4 Flowspec address family view
BGP-VPN IPv4 Flowspec address family view
BGP IPv6 Flowspec address family view
BGP-VPN IPv6 Flowspec address family view

Change description

The BGP IPv6 Flowspec address family view and BGP-VPN IPv6 Flowspec address family view are added, and the following parameters are added:

ipv6-address: Specifies a peer by its IPv6 address.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, the device does not change the next hop of routes advertised to all dynamic peers in the subnet.

Modified command: policy vpn-target

Syntax

```
policy vpn-target  
undo policy vpn-target
```

Old views

BGP VPNv4 Flowspec address family view

New views

BGP VPNv4 Flowspec address family view
BGP VPNv6 Flowspec address family view

Change description

The BGP VPNv6 Flowspec address family view is added.

New command: redirect ip recursive-lookup tunnel

Use **redirect ip recursive-lookup tunnel** to enable recursion to tunnels for Flowspec rules with an action of redirecting to a next hop.

Use **undo redirect ip recursive-lookup tunnel** to restore the default.

Syntax

```
redirect ip recursive-lookup tunnel [ tunnel-selector tunnel-selector-name ]  
undo redirect ip recursive-lookup tunnel
```

Default

Recursion to tunnels is disabled for Flowspec rules with an action of redirecting to a next hop.

Views

BGP IPv4 Flowspec address family view

BGP IPv6 Flowspec address family view

Predefined user roles

network-admin

Parameters

tunnel-selector *tunnel-selector-name*: Specifies a tunnel selector by its name, a case-sensitive string of 1 to 40 characters. If you do not specify a tunnel selector, the device uses the default tunnel selection order to select tunnels. For information about route recursion, see BGP configuration in *Layer 3—IP Routing Configuration Guide*. For information about tunnel selectors, see tunnel policy configuration in *MPLS Configuration Guide*.

Examples

Enable recursion to tunnels for IPv4 Flowspec rules with an action of redirecting to a next hop.

```
<Sysname> system-view
```

```
[Sysname] bgp 200
```

```
[Sysname-bgp-default] address-family ipv4 flowspec
```

```
[Sysname-bgp-default-flowspec-ipv4] redirect ip recursive-lookup tunnel tunnel-selector  
bgp
```

Modified command: reflect between-clients

Syntax

reflect between-clients

undo reflect between-clients

Old views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP VPNv4 Flowspec address family view

New views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP VPNv4 Flowspec address family view

BGP IPv6 Flowspec address family view

BGP-VPN IPv6 Flowspec address family view

BGP VPNv6 Flowspec address family view

Change description

The BGP IPv6 Flowspec address family view, BGP-VPN IPv6 Flowspec address family view, and BGP VPNv6 Flowspec address family view are added.

Modified command: reflector cluster-id

Syntax

reflector cluster-id { *cluster-id* | *ipv4-address* }

undo reflector cluster-id

Old views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP VPNv4 Flowspec address family view

New views

BGP IPv4 Flowspec address family view

BGP-VPN IPv4 Flowspec address family view

BGP VPNv4 Flowspec address family view

BGP IPv6 Flowspec address family view

BGP-VPN IPv6 Flowspec address family view

BGP VPNv6 Flowspec address family view

Change description

The BGP IPv6 Flowspec address family view, BGP-VPN IPv6 Flowspec address family view, and BGP VPNv6 Flowspec address family view are added.

Modified command: reset flow-route statistics

Old syntax

reset flow-route statistics { **all** | *flow-route-id* | **ip** [**vpn-instance** *vpn-instance-name*] }

New syntax

reset flow-route statistics { **all** | { **ip** | **ipv6** } [**all** | **vpn-instance** *vpn-instance-name*] | *flow-route-id* }

Views

User view

Change description

The following parameter is added:

ipv6: Specifies IPv6 Flowspec rules.

Modified command: vpn-target

Syntax

vpn-target *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

Old views

VPN instance view

VPN instance IPv4 Flowspec family address view

New views

VPN instance view

VPN instance IPv4 Flowspec family address view

VPN instance IPv6 Flowspec family address view

Change description

The VPN instance IPv6 Flowspec family address view is added.

New feature: MP packet fast forwarding

Configuring MP packet fast forwarding

About this task

With MP packet fast forwarding enabled on an interface, the packets sent out of the interface do not carry the MP sequence number or fragment ID. Each packet is sent as a whole to improve the forwarding efficiency.

Procedure

1. Enter system view.
system-view
2. Enter VT interface view.
interface virtual-template *number*
3. Enable MP packet fast forwarding.
ppp mp fast-forward enable

Command reference

New command: ppp mp fast-forward enable

Use **ppp mp fast-forward enable** to enable MP packet fast forwarding.

Use **undo ppp mp fast-forward enable** to disable MP packet fast forwarding.

Syntax

ppp mp fast-forward enable

undo ppp mp fast-forward enable

Default

MP packet fast forwarding is disabled.

Views

VT interface view

Dialer interface view

MP-group interface view

Predefined user roles

network-admin

Usage guidelines

With MP packet fast forwarding enabled on an interface, the packets sent out of the interface do not carry the MP sequence number or fragment ID. Each packet is sent as a whole to improve the forwarding efficiency.

With the **ppp mp fast-forward enable** command executed on an interface, the **ppp mp fragment disable** command on the interface does not take effect.

Examples

```
# Enable MP packet fast forwarding on MP-group 2/0/0.
<Sysname> system-view
[Sysname] interface mp-group 2/0/0
[Sysname-MP-group2/0/0] ppp mp fast-forward enable
```

Related commands

ppp mp fragment disable

New feature: Setting the traffic statistics update timer for IPoE sessions

Setting the traffic statistics update timer for IPoE sessions

About this task

Perform this task to set the traffic statistic update timer for IPoE sessions.

Procedure

1. Enter system view.
system-view
2. Set the traffic statistics update timer for IPv4 IPoE sessions.
ip subscriber timer traffic *value*
By default, the traffic statistics update timer for IPv4 IPoE sessions is 60000 milliseconds.
3. Set the traffic statistics update timer for IPv6 IPoE sessions.
ipv6 subscriber timer traffic *value*
By default, the traffic statistics update timer for IPv6 IPoE sessions is 60000 milliseconds.

Command reference

New command: ip subscriber timer traffic

Use **ip subscriber timer traffic** to set the traffic statistics update timer for IPv4 IPoE sessions.

Use **undo ip subscriber timer traffic** to restore the default.

Syntax

```
ip subscriber timer traffic value
undo ip subscriber timer traffic value
```

Default

The traffic statistics update timer for IPv4 IPoE sessions is 60000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the traffic statistics update timer for IPv4 IPoE sessions, a multiple of 100 in the range of 100 to 1200000 milliseconds.

Usage guidelines

When the timer times out, IPoE updates traffic statistics for static and dynamic IPv4 IPoE sessions.

Examples

```
# Set the traffic statistics update time for IPv4 IPoE sessions to 300 milliseconds.  
<Sysname> system-view  
[Sysname] ip subscriber timer traffic 300
```

New command: ipv6 subscriber timer traffic

Use **ipv6 subscriber timer traffic** to set the traffic statistics update timer for IPv6 IPoE sessions.

Use **undo ipv6 subscriber timer traffic** to restore the default.

Syntax

```
ipv6 subscriber timer traffic value  
undo ipv6 subscriber timer traffic value
```

Default

The traffic statistics update timer for IPv6 IPoE sessions is 60000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the traffic statistics update timer for IPv6 IPoE sessions, a multiple of 100 in the range of 100 to 1200000 milliseconds.

Usage guidelines

When the timer times out, IPoE updates traffic statistics for static and dynamic IPv6 IPoE sessions.

Examples

```
# Set the traffic statistics update time for IPv6 IPoE sessions to 300 milliseconds.  
<Sysname> system-view  
[Sysname] ipv6 subscriber timer traffic 300
```

New feature: Configuring the time interval for traffic rate calculation of portal users

Configuring the time interval for traffic rate calculation of portal users

About this task

By default, the device calculates the portal user traffic rate per second to obtain the instantaneous traffic rate of the users. For more accurate and effective analysis of the user traffic, you can perform this task to specify a longer time interval to calculate the average traffic rate. The device divides the total user traffic obtained in the specified time interval by the time interval to get the average traffic rate. To view the average traffic rate of portal users, use the **display portal user** command.

Procedure

1. Enter system view.
system-view
2. Configure the time interval for traffic rate calculation of portal users.
portal traffic-rate statistics-interval *interval*

By default, the time interval for traffic rate calculation of portal users is 1 second.

Command reference

New command: portal traffic-rate statistics-interval

Use **portal traffic-rate statistics-interval** to configure the time interval for traffic rate calculation of portal users.

Use **undo portal traffic-rate statistics-interval** to restore the default.

Syntax

portal traffic-rate statistics-interval *interval*

undo portal traffic-rate statistics-interval

Default

The time interval for traffic rate calculation of portal users is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the time interval for traffic rate calculation of portal users, in the range of 1 to 3600 seconds.

Usage guidelines

By default, the device calculates the portal user traffic rate per second to obtain the instantaneous traffic rate of the users. For more accurate and effective analysis of the user traffic, you can use this command to specify a longer time interval to calculate the average traffic rate. The device divides the total user traffic obtained in the specified time interval by the time interval to get the average traffic rate. To view the average traffic rate of portal users, use the **display portal user** command.

Examples

Set the time interval for traffic rate calculation of portal users to 10 seconds.

```
<Sysname> system-view
```

```
[Sysname] portal traffic-rate statistics-interval 10
```

Related commands

display portal user

Modified command: display portal user

Syntax

display portal user { **all** | **ap** *ap-name* [**radio** *radio-id*] } | **auth-type** { **cloud** | **email** | **facebook** | **local** | **mac-trigger** | **normal** | **qq** | **wechat** } | **interface** *interface-type* *interface-number* | **ip** *ipv4-address* | **ipv6** *ipv6-address* | **mac** *mac-address* | **pre-auth** [**interface** *interface-type* *interface-number* | **ip** *ipv4-address* | **ipv6** *ipv6-address*] | **username** *username* } [**brief** | **verbose**]

Views

Any view

Change description

After modification, when you specify the **verbose** keyword to display detailed information about portal users, the following fields are displayed in the output for this command:

Field	Description
Traffic average rate	Average traffic rate statistics for the portal user.
Uplink rate	Average rate of the upstream traffic in bytes per second.
Downlink rate	Average rate of the downstream traffic in bytes per second.

New feature: Disabling sending a specific type of ICMP messages

Disabling sending a specific type of ICMP messages

About this task

By default, the device sends all types of ICMP messages except Destination Unreachable, Time Exceeded, and Redirect messages. Attackers might obtain information from specific types of ICMP messages, causing security issues.

For security purposes, you can perform this task to disable sending ICMP messages of specific types.

Restrictions and guidelines

Disabling sending ICMP messages of a specific type might affect network operation. Please use this feature with caution.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following tasks:

- Execute the **ip icmp send enable** command.
- Execute one of the following commands as needed:
 - **ip unreachable enable**
 - **ip ttl-expires enable**
 - **ip redirects enable**

Procedure

1. Enter system view.

system-view

2. Disable the device from sending a specific type of ICMP messages.

undo ip icmp { name *icmp-name* | type *icmp-type* code *icmp-code* } send enable

By default, the device sends all types of ICMP messages except Destination Unreachable, Time Exceeded, and Redirect messages

Command reference

ip icmp send enable

Use **ip icmp send enable** to enable the device to send a specific type of ICMP messages.

Use **undo ip icmp send enable** to disable the device from sending a specific type of ICMP messages.

Syntax

ip icmp { name *icmp-name* | type *icmp-type* code *icmp-code* } send enable

undo ip icmp { name *icmp-name* | type *icmp-type* code *icmp-code* } send enable

Default

The device sends all types of ICMP messages except Destination Unreachable, Time Exceeded, and Redirect messages.

Views

System view

Predefined user roles

network-admin

Parameters

name *icmp-name*: Specifies an ICMP message name, a case-insensitive string of 1 to 20 characters.

type *icmp-type*: Specifies an ICMP message type. The value range for the *icmp-type* argument is 0 to 255.

code *icmp-code*: Specifies an ICMP message code. The value range for the *icmp-code* argument is 0 to 255.

Usage guidelines



CAUTION:

Disabling sending ICMP messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device sends all types of ICMP messages except Destination Unreachable, Time Exceeded, and Redirect messages. Attackers might obtain information from specific types of ICMP messages, causing security issues.

For security purposes, you can use this command to disable the device from sending ICMP messages of specific types.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following tasks:

- Execute the **ip icmp send enable** command.
- Execute one of the following commands as needed:
 - **ip unreachable enable**
 - **ip ttl-expires enable**
 - **ip redirects enable**

Table 25 shows common ICMP messages and their meanings.

Table 25 Common ICMP messages

Name	Type	Code	Description
echo	8	0	Echo request used to ping a target node.
echo-reply	0	0	Echo reply sent by a target node after receiving an echo request.
fragmentneed-dfset	3	4	Packets that need fragmentation but have the DF bit set.
host-redirect	5	1	Host redirection.
host-tos-redirect	5	3	Host ToS redirection.
host-unreachable	3	1	Unreachable host.
information-reply	16	0	Information reply.
information-request	15	0	Information request.
net-redirect	5	0	Network redirection.
net-tos-redirect	5	2	Network ToS redirection.
net-unreachable	3	0	Unreachable network.
parameter-problem	12	0	Invalid parameter.
port-unreachable	3	3	Unreachable port.
protocol-unreachable	3	2	Unreachable protocol.
reassembly-timeout	11	1	Fragment reassembly timeout.
source-quench	4	0	Source quench message.
source-route-failed	3	5	Source route failure.
timestamp-reply	14	0	Timestamp reply.
timestamp-request	13	0	Timestamp request.
ttl-exceeded	11	0	TTL exceeded in transit.

Examples

```
# Enable the device to send ICMP echo reply messages.  
<Sysname> system-view  
[Sysname] ip icmp name echo-reply send enable
```

Related commands

```
ip icmp fragment discarding  
ip redirects enable  
ip ttl-expires enable  
ip unreachable enable
```

New feature: Disabling receiving a specific type of ICMP messages

Disabling receiving a specific type of ICMP messages

About this task

By default, the device receives all types of ICMP messages. Such a setting might affect device performance if a large number of ICMP responses are received within a short time. To resolve this issue, you can perform this task to disable the device from receiving a specific type of ICMP messages.

Restrictions and guidelines

Disabling receiving ICMP messages of a specific type might affect network operation. Please use this feature with caution.

Procedure

1. Enter system view.
system-view
2. Disable the device from receiving a specific type of ICMP messages.
undo ip icmp { name *icmp-name* | type *icmp-type* code *icmp-code* } receive enable
By default, the device receives all types of ICMP messages.

Command reference

ip icmp receive enable

Use **ip icmp receive enable** to enable the device to receive a specific type of ICMP messages.

Use **undo ip icmp receive enable** to disable the device from receiving a specific type of ICMP messages.

Syntax

```
ip icmp { name icmp-name | type icmp-type code icmp-code } receive enable  
undo ip icmp { name icmp-name | type icmp-type code icmp-code } receive enable
```

Default

The device can receive all types of ICMP messages.

Views

System view

Predefined user roles

network-admin

Parameters

name *icmp-name*: Specifies an ICMP message name, a case-insensitive string of 1 to 20 characters.

type *icmp-type*: Specifies an ICMP message type. The value range for the *icmp-type* argument is 0 to 255.

code *icmp-code*: Specifies an ICMP message code. The value range for the *icmp-code* argument is 0 to 255.

Usage guidelines



CAUTION:

Disabling receiving ICMP messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device receives all types of ICMP messages. Such a setting might affect device performance if a large number of ICMP responses are received within a short time. To solve this issue, you can use this command to disable the device from receiving a specific type of ICMP messages.

Table 26 shows common ICMP messages and their meanings.

Table 26 Common ICMP messages

Name	Type	Code	Description
echo	8	0	Echo request used to ping a target node.
echo-reply	0	0	Echo reply sent by a target node after receiving an echo request.
fragmentneed-dfset	3	4	Packets that need fragmentation but have the DF bit set.
host-redirect	5	1	Host redirection.
host-tos-redirect	5	3	Host ToS redirection.
host-unreachable	3	1	Unreachable host.
information-reply	16	0	Information reply.
information-request	15	0	Information request.
net-redirect	5	0	Network redirection.
net-tos-redirect	5	2	Network ToS redirection.
net-unreachable	3	0	Unreachable network.
parameter-problem	12	0	Invalid parameter.
port-unreachable	3	3	Unreachable port.
protocol-unreachable	3	2	Unreachable protocol.
reassembly-timeout	11	1	Fragment reassembly timeout.

Name	Type	Code	Description
source-quench	4	0	Source quench message.
source-route-failed	3	5	Source route failure.
timestamp-reply	14	0	Timestamp reply.
timestamp-request	13	0	Timestamp request.
ttl-exceeded	11	0	TTL exceeded in transit.

Examples

Enable the device to receive ICMP echo reply messages.

```
<Sysname> system-view
```

```
[Sysname] ip icmp name echo-reply receive enable
```

New feature: Display the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state

Displaying the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state

Use **display link-aggregation troubleshooting** to display the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state.

Command reference

display link-aggregation troubleshooting

Use **display link-aggregation troubleshooting** to display the aggregation states of aggregation member ports and the reason why a port was placed in Unselected state.

Syntax

```
display link-aggregation troubleshooting [ { bridge-aggregation | route-aggregation }  
[ interface-number ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

bridge-aggregation: Specifies Layer 2 aggregate interfaces.

route-aggregation: Specifies Layer 3 aggregate interfaces.

interface-number: Specifies an existing aggregate interface by its number.

Usage guidelines

If you do not specify an aggregate interface type, the command displays information about all aggregation groups.

If you specify an aggregate interface type but do not specify an interface number, the command displays information about all aggregation groups of the specified type.

You can specify the **bridge-aggregation** or **route-aggregation** keyword only when aggregate interfaces of the specified type exist on the device.

Examples

Display the aggregation states of aggregation member ports for all aggregation groups and the reason why a port was placed in Unselected state.

```
<Sysname> display link-aggregation troubleshooting
Aggregate Interface: Bridge-Aggregation2
Member ports:
  GE1/0/2
    Status: Selected
  GE1/0/3
    Status: Unselected
    Reason: The physical or line protocol state of the port is down
    Advice: Check the connection
```

Table 27 Command output

Field	Description
Aggregate interface	Name of the aggregate interface.
Member ports	Information of aggregation member ports.
Status	Port state: • Selected. • Unselected.
Reason	Reason why the port was placed in Unselected state. For more information, see Table 28
Advice	Recommended action. For more information, see Table 29

Table 28 Reason

Field
The number of Selected ports had reached the upper limit
Hardware resources were not enough
The number of Selected ports was below the lower limit
The link aggregation configuration of the port was incorrect
The link aggregation configuration of its peer port was incorrect

The physical or line protocol state of the port was down
The port's hardware restriction prevented it from being Selected
The speed configuration of the port was different from that of the reference port
The duplex mode of the port was different from that of the reference port
The port and the aggregate interface had different attribute configurations
The BFD session state of the port was down
No LACPDU was received by the reference port
The reference port received its own LACPDUs
The link of the port was not aggregatable
The link of the peer port was not aggregatable
The card that hosts the port was absent
The port's operational key was invalid
Link-aggregation traffic redirection was triggered on the local port
The port had not received LACPDUs
The operational key of the peer port was different from that of the reference port
Link-aggregation traffic redirection was triggered on the peer port
The system MAC address of the peer port was different from that of the peer port for the reference port
The peer port did not have the Synchronization flag
The port was in Standby state

Table 29 Advice

Field
Modify the aggregation group configuration
Release resources
Modify port configuration
Modify peer port configuration
Check the connection
Use another port
Change the port rate to be the same as that of the reference port
Change the port duplex mode to be the same as that of the reference port
Change the port attribute configuration to be the same as that of the aggregate interface
Check the link that conveys the BFD session
Check whether the peer sends LACPDUs correctly
Check whether the device has a loop
Make sure the card that hosts the port is installed
Check whether the port sends LACPDUs correctly
Change the peer system MAC address to be the same as that of the reference port

Check the LACPDUs sent by the peer
Please check the aggregation state of member ports in a few minutes

New feature: Python2 progress monitoring

Feature description

As from this release, the third-party progress monitoring feature (enabled by executing the **third-part-process start** command) supports monitoring Python2 progress.

New feature

New feature: Software upgrade through CWMP

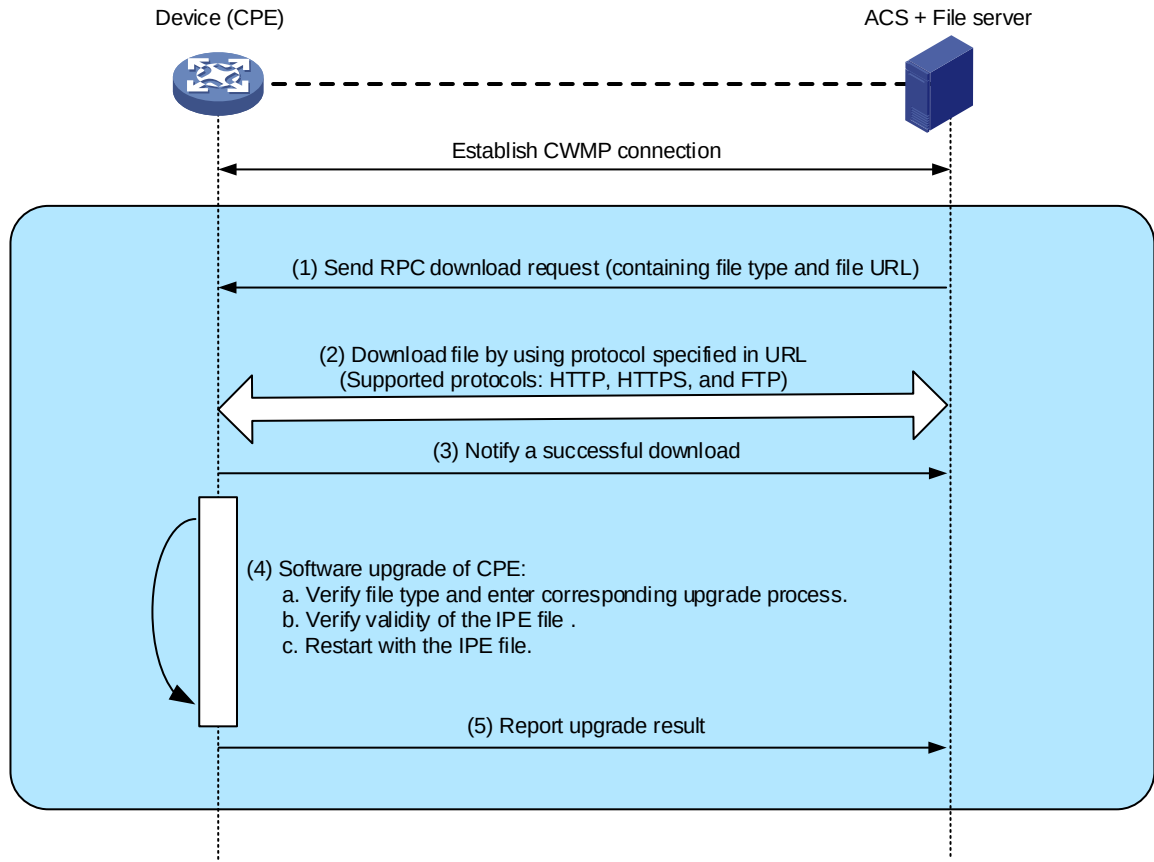
Software upgrade through CWMP

To perform software upgrade through CWMP, save the firmware upgrade image (an IPE file) on the file server. The ACS will request the CPE to download the file at a specific URL for software upgrade.

As shown in [Figure 1](#), CWMP software upgrade operates as follows:

1. The ACS sends an RPC request to the CPE and requests the CPE to download the image. The request specifies file type 1 (indicating a firmware upgrade image) and the file URL.
2. The CPE parses the received URL that carries the protocol type and file name and downloads the IPE file from the specified file server. You can deploy the file server and the ACS on the same physical device or on different physical devices.
3. After the IPE file is downloaded, the CPE notifies the ACS of a successful download.
4. The CPE uses the downloaded IPE file to upgrade the software as follows:
 - a. Enters the software upgrade process based on file type 1.
 - b. Verifies the validity of the IPE file.
 - c. For a valid IPE file, to avoid insufficient media storage space caused by direct decompression of the IPE file, the CPE operates as follows:
 - If the BIN file in the IPE file uses the same name as the BIN file used at this startup, the CPE decompresses the IPE file and replaces the local BIN file with the new BIN file.
 - If the BIN file names are different, the CPE deletes the backup next-startup software image to release space and then decompresses the IPE file. Then, the CPE sets the new BIN file as the primary software image for next startup and sets the BIN file used at this startup as the backup software image for the next startup.
5. The CPE restarts automatically for the downloaded IPE file to take effect.

Figure 1 Software upgrade through CWMP



New feature: Specifying a CPE service port number

Specifying a CPE service port number

About this task

Perform this task to configure a CPE service port number. When the ACS initiates a connection to the CPE, the ACS must provide the same port number as configured on the CPE for a successful connection. After the command is configured, the CPE uses the new port to provide services and the CPE services created before the configuration are not affected.

Procedure

1. Enter system view.
system-view
2. Enter CWMP view.
cwmp
3. Specify a CPE service port number.
cwmp cpe port port

By default, the CPE service port number is 7547.

Command reference

cwmp cpe port

Use **cwmp cpe port** to specify a CPE service port number.

Use **undo cwmp cpe port** to restore the default.

Syntax

cwmp cpe port *port*

undo cwmp cpe port *port*

Default

The CPE service port number is 7547.

Views

CWMP view

Predefined user roles

network-admin

Parameters

port: Specifies a CPE service port number in the range of 1000 to 65535.

Usage guidelines

Perform this task to configure a CPE service port number. When the ACS initiates a connection to the CPE, the ACS must provide the same port number as configured on the CPE for a successful connection. After the command is configured, the CPE uses the new port to provide services and the CPE services created before the configuration are not affected.

Examples

Specify port 51703 to provide CPE services.

```
<Sysname> system
```

```
[Sysname] cwmp
```

```
[Sysname-cwmp] cwmp cpe port 51703
```

New feature: Configuring the notification format and enabling notifications to carry the device serial number (SN)

Configuring the notification format and enabling notifications to carry the device serial number

Procedure

1. Enter system view.
system-view
2. (Optional.) Specify the notification format as CMCC.

snmp-agent trap format cmcc

By default, the notifications are in standard format.

3. (Optional.) Enable notifications to carry the device serial number.

snmp-agent trap withsn

By default, the notifications do not carry the device serial number.

Command reference

snmp-agent trap format

Use **snmp-agent trap format** to specify the format for the notifications sent to the NMS.

Use **undo snmp-agent trap format** to restore the default.

Syntax

snmp-agent trap format cmcc

undo snmp-agent trap format

Default

The notifications are in standard format.

Views

System view

Predefined user roles

network-admin

Parameters

cmcc: Specifies the CMCC format.

Usage guidelines

You can select the standard or CMCC format for notifications sent to an NMS as needed.

Examples

Specify the CMCC format for the notifications sent to the NMS.

<Sysname> system-view

[Sysname] snmp-agent trap format cmcc

snmp-agent trap withsn

Use **snmp-agent trap withsn** to enable the notifications to carry the device serial number (SN).

Use **undo snmp-agent trap withsn** to restore the default.

Syntax

snmp-agent trap withsn

undo snmp-agent trap withsn

Default

The notifications do not carry the device SN.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After this command is configured, the notifications sent from the device to the NMS carry the device SN that identifies the device uniquely.

Examples

Enable the notifications to carry the device SN.

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap withsn
```

New feature: Configuring SQA

About this task

Service quality analysis (SQA) enables the device to identify SIP- or H.323-based multimedia traffic and preferentially forward this traffic to ensure multimedia service quality. Use this feature to decrease multimedia stuttering and improve user experience.

Restrictions: Hardware compatibility with SQA

Hardware	SQA compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR 2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	Yes

Hardware	SQA compatibility
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	Yes
MSR3610-G, MSR3620-G	Yes
MSR3640-G	Yes
MSR3640-X1-HI	Yes

Hardware	SQA compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	SQA compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	Yes
MSR3610-IE-XS	Yes
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	SQA compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No

Hardware	SQA compatibility
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Restrictions and guidelines: SQA configuration

SQA does not support analysis of encrypted SIP or H.323 protocol packets.

Configuring SIP-based SQA

Restrictions and guidelines

Make sure SQA uses different port numbers to listen for SIP and H.323 packets.

Procedure

1. Enter system view.
system-view
2. Enter SQA view.
sqa
3. Enable SIP-based SQA.
sqa-sip enable
By default, SIP-based SQA is disabled.

Configuring H.323-based SQA

Restrictions and guidelines

Make sure SQA uses different port numbers to listen for SIP and H.323 packets.

Procedure

1. Enter system view.
system-view
2. Enter SQA view.
sqa
3. Enable H.323-based SQA.
sqa-h323 enable
By default, H.323-based SQA is disabled.

Display and maintenance commands for SQA

Execute **display** commands in any view.

Task	Command
Display SIP or H.323 call information.	display sqa { h323 sip } call [[call-id <i>call-id</i>] verbose]
Display SIP or H.323 call statistics.	display sqa { h323 sip } call-statistics

Command reference

display sqa call

Use **display sqa { h323 | sip } call** to display SIP call information.

Syntax

display sqa { h323 | sip } call [[call-id *call-id*] verbose]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

h323: Specifies H.323 calls.

sip: Specifies SIP calls.

call-id *call-id*: Specifies a SIP or H.323 call by its call ID, a case-insensitive string of 1 to 64 characters. If you do not specify a SIP or H.323 call, this command displays information for all SIP or H.323 calls.

verbose: Displays detailed information about a SIP or H.323 call.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all SIP or H.323 calls.

The CPU might be overwhelmed by too many SIP calls and fail to process all packets. In this case, the caller or callee information will be displayed as 0.0.0.0:0.

Examples

Display brief information about all SIP calls.

```
<Sysname> display sqa sip call
```

```

Caller                               Callee                               Call ID
192.168.111.222:65000 192.168.111.223:5000  asdlkfjakdjfkl
192.121.111.252:65012 192.171.251.223:5000  adfdffjakdjfkl
```

Table 30 Command output

Field	Description
Caller	IP address and port number of the calling party.
Callee	IP address and port number of the called party.

Field	Description
Call ID	ID of a SIP call, which uniquely identifies the call.

Display detailed information about a SIP call.

```
<Sysname> display sqa sip call call-id asdlkfjakdjfkl verbose
```

```
Call ID: asdlkfjakdjfkl
```

```
Caller information:
```

```
IP: 192.168.111.222    Port: 65000    MAC: 0011-2233-CD55
```

```
Tag: 1111@192.168.10.1
```

```
Callee information:
```

```
IP: 192.168.111.123    Port: 65000    MAC: 0111-2AB3-4456
```

```
Tag: 2222@192.168.10.2
```

```
Type: Audio    VLAN: 1024    StartTime: 2019-10-12 14:21:36
```

```
MOS(F): 3    MOS(R): 3
```

```
Forward flow (octets): 123564    Forward flow (packets): 456215
```

```
Reverse flow (octets): 25642354    Reverse flow (packets): 2451235
```

Table 31 Command output

Field	Description
Call ID	ID of the call, which uniquely identifies the call.
IP	IP address of the calling party or called party.
Port	Port number of the calling party or called party.
MAC	MAC address of the calling party or called party.
Tag	Tag of the calling party or called party. The tag is a URL in the format of <i>x@y</i> , where <i>x</i> represents the username or phone number and <i>y</i> represents the domain name or address of the proxy server.
Type	Media type: - Audio. - Video.
VLAN	ID of the VLAN to which the SIP call belongs. This field displays a hyphen (-) if data of the SIP call is transmitted by the device through a Layer 3 routing interface.
StartTime	Time when the SIP call was established.
MOS(F)	Mean Opinion Score (MOS) value for the originating voice traffic (traffic from the calling party to the called party). The higher the value, the better the service. This field displays a hyphen (-) if the system fails to obtain the value.
MOS(R)	MOS value for the returning voice traffic (traffic from the called party to the calling party). The higher the value, the better the service. This field displays a hyphen (-) if the system fails to obtain the value.
Forward flow (octets)	Statistics of the originating voice traffic, in bytes.
Forward flow (packets)	Statistics of the originating voice traffic, in packets.
Reverse flow (octets)	Statistics of the returning voice traffic, in bytes.

Field	Description
Reverse flow (packets)	Statistics of the returning voice traffic, in packets.

Display brief information about all H.323 calls.

```
<Sysname> display sqa h323 call
```

Caller	Callee	Call ID
192.168.111.222:65000	192.168.111.223:5000	3e33ecbd-6f1d-1910-8b52-6805ca5d1208
192.121.111.252:65012	192.171.251.223:5000	42910c03-e31c-1910-9a63-000c29209aa9

Table 32 Command output

Field	Description
Caller	IP address and port number of the calling party.
Callee	IP address and port number of the called party.
Call ID	ID of an H.323 call, which uniquely identifies the call.

Display detailed information about an H.323 call.

```
<Sysname> display sqa h323 call call-id 3e33ecbd-6f1d-1910-8b52-6805ca5d1208 verbose
```

```
Call ID: 3e33ecbd-6f1d-1910-8b52-6805ca5d1208
```

```
Caller information:
```

```
IP: 192.168.111.222    Port: 65000    MAC: 0011-2233-CD55
```

```
Callee information:
```

```
IP: 192.168.111.123    Port: 65000    MAC: 0111-2AB3-4456
```

```
GUID: 42910c03-e31c-1910-9a62-000c29209aa9
```

```
Protocol: TCP(6)
```

```
Session ID: 2
```

```
Type: Audio          Vlan: 1          StartTime: 2020-03-04 13:57:53
```

```
MOS(F): 3           MOS(R): 3
```

```
Forward flow (octets): 123564          Forward flow (packets): 456215
```

```
Reverse flow (octets): 25642354        Reverse flow (packets): 2451235
```

Table 33 Command output

Field	Description
Call ID	ID of the call, which uniquely identifies the call.
IP	IP address of the calling party or called party.
Port	Port number of the calling party or called party.
MAC	MAC address of the calling party or called party.
GUID	Global unified identifier that uniquely identifies the H.323 call.
Protocol	Protocol type and number: - TCP. - UDP.
Session ID	Session ID of the H.323 call.
Type	Media type: Audio.

Field	Description
	Video.
VLAN	ID of the VLAN to which the H.323 call belongs.
StartTime	Time when the H.323 call was established. This field displays a hyphen (-) if data of the SIP call is transmitted by the device through a Layer 3 routing interface.
MOS(F)	Mean Opinion Score (MOS) value for the originating voice traffic (traffic from the calling party to the called party). The higher the value, the better the service. This field displays a hyphen (-) if the system fails to obtain the value.
MOS(R)	MOS value for the returning voice traffic (traffic from the called party to the calling party). The higher the value, the better the service. This field displays a hyphen (-) if the system fails to obtain the value.
Forward flow (octets)	Statistics about the originating voice traffic, in bytes.
Forward flow (packets)	Statistics about the originating voice traffic, in packets.
Reverse flow (octets)	Statistics about the returning voice traffic, in bytes.
Reverse flow (packets)	Statistics about the returning voice traffic, in packets.

Related commands

sqa-h323 enable

sqa-sip enable

display sqa call-statistics

Use **display sqa { h323 | sip } call-statistics** to display SIP call statistics.

Syntax

display sqa { h323 | sip } call-statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

h323: Specifies H.323 calls.

sip: Specifies SIP calls.

Examples

Display H.323 call statistics.

```
<Sysname> display sqa h323 call-statistics
Total calls      : 21
Successful calls : 15 (Active: 10)
Timeout calls    : 2
Abnormal calls   : 3
```


Display SIP call statistics.

```
<Sysname> display sqa sip call-statistics
Total calls      : 21
Successful calls : 15 (Active: 10)
Timeout calls    : 2
Abnormal calls   : 3
```

Table 34 Command output

Field	Description
Total calls	Total number of calls that have been placed.
Successful calls	Total number of calls that have been established successfully.
Active	Total number of ongoing calls.
Timeout calls	Total number of timeout calls.
Abnormal calls	Total number of abnormal calls.

Related commands

sqa-h323 enable

sqa-sip enable

sqa

Use **sqa** to enter server quality analysis (SQA) view.

Syntax

sqa

Views

System view

Predefined user roles

network-admin

Examples

Enter SQA view.

```
<Sysname> system-view
[Sysname] sqa
[Sysname-sqa]
```

sqa-h323 enable

Use **sqa-h323 enable** to enable H.323-based SQA.

Use **undo sqa-h323 enable** to disable H.323-based SQA.

Syntax

sqa-h323 enable

undo sqa-h323 enable

Default

H.323-based SQA is disabled.

Views

SQA view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to preferentially forward H.323-based multimedia traffic and analyze the traffic to improve multimedia service quality.

SQA does not support analysis of encrypted H.323 protocol packets or fragments.

Examples

```
# Enable H.323-based SQA.
<Sysname> system-view
[Sysname] sqa
[Sysname-sqa] sqa-h323 enable
```

sqa-sip enable

Use **sqa-sip enable** to enable SIP-based SQA.

Use **undo sqa-sip enable** to disable SIP-based SQA.

Syntax

sqa-sip enable
undo sqa-sip enable

Default

SIP-based SQA is disabled.

Views

SQA view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to preferentially forward SIP-based multimedia traffic and analyze the traffic to improve multimedia service quality.

SQA does not support analysis of encrypted SIP protocol packets or fragments.

Examples

```
# Enable SIP-based SQA.
<Sysname> system-view
[Sysname] sqa
[Sysname-sqa] sqa-sip enable
```

New feature: Specifying the number of CPU cores allocated as control cores

Specifying the number of CPU cores as control cores

About this task

Control cores are used for the system services on the control plane. Typically, all services are running in one CPU core. If services need a large amount of computing, such as for a VPN with device networking, using only one CPU core might affect computing speed. In this case, you can use this feature to increase the number of control cores.

You can use **display core allocation** to obtain information about CPU core allocation.

Hardware and feature compatibility

Hardware	Feature compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR 2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR 3610, MSR 3620, MSR 3620-DP, MSR	No

3640, MSR 3660	
MSR3610-G, MSR3620-G	No
MSR3640-X1-HI	Yes

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Feature compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	Yes

Hardware	Feature compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Restrictions and guidelines

The total number of CPU cores that are allocated must be equal to or smaller than the total number of CPU cores on the device.

For the configuration to take effect, restart the slot where CPU cores reside.

Procedure

1. Enter system view.

system-view

2. Specify the number of CPU cores allocated as control cores.

In standalone mode:

allocate core control-core *core-count*

In IRF mode:

allocate core slot *slot-number* **control-core** *core-count*

By default, the number of CPU cores as control cores is 1.

Command reference

allocate core

Use **allocate core** to specify the number of CPU cores allocated as control cores.

Syntax

In standalone mode:

allocate core control-core *core-count*

undo allocate core

In IRF mode:

allocate core slot *slot-number* **control-core** *core-count*

undo allocate core slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No

Hardware	Command compatibility
MSR2600-10-X1	No
MSR 2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR 3610, MSR 3620, MSR 3620-DP, MSR 3640, MSR 3660	No
MSR3610-G, MSR3620-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No

Hardware	Command compatibility
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

The number of CPU cores allocated as control cores is 1.

Views

System view

Predefined user roles

network-admin
network-operator

Parameters

control-core *core-count*: Specify the number of CPU cores as control cores.

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Usage guidelines

The total number of CPU cores that are allocated must be equal to or smaller than the total number of CPU cores on the device.

Control cores are used for the system services on the control plane. Typically, all services are running in one CPU core. If services need a large amount of computing, such as for a VPN with device networking, one CPU core might affect computing speed. In this case, you can use this command to increase the number of control cores.

For the configuration to take effect, restart the slot where CPU cores reside.

Examples

```
# (In IRF mode.) Specify the number of CPU cores allocated as control cores.
<Sysname> system-view
[Sysname] allocate core slot 1 control-core 4
Are you sure you want to change the allocation of CPU cores? [Y/N]:y
The configuration will take effect after the card restarts.
```

Related commands

display core allocation

display core allocation

Use **display core allocation** to display information about CPU core allocation.

Syntax

In standalone mode:

display core allocation

In IRF mode:

display core allocation slot *slot-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR 2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR 3610, MSR 3620, MSR 3620-DP,	No

Hardware	Command compatibility
MSR 3640, MSR 3660	
MSR3610-G, MSR3620-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No

Hardware	Command compatibility
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Examples

(In standalone mode.) Display information about CPU core allocation.

```
<Sysname> display core allocation
```

Control cores:

Current: 0

Next startup: 0-3

Data cores:

Current: 1-15

Next startup: 4-15

Table 35 Command output

Field	Description
Control cores	Control core information.
Current	Number list of CPU cores that are used as control cores.
Next startup	Number list of CPU cores that will be used as control cores at next startup.
Data cores	Data core information.
Current	Number list of CPU cores that are used as data cores.
Next startup	Number list of CPU cores that will be used as data cores at next startup.

Related commands

allocate core

New feature: Enabling the capability of MPLS BFD to trigger tunnel-down

Enable the capability of MPLS BFD to trigger tunnel-down

1. Enter system view.

- system-view**
2. Enable BFD for MPLS.
mpls bfd enable
 By default, BFD for MPLS is disabled.
 3. (Optional.) Enable the capability of MPLS BFD to trigger tunnel-down.
 - a. Enter MPLS TE view.
mpls te
 - b. Enable the capability of MPLS BFD to trigger tunnel-down.
mpls bfd trigger tunnel-down enable
 By default, MPLS BFD is able to trigger tunnel-down.
 If you configure static MPLS BFD in a primary/backup scenario, the device creates a BFD session for only the primary path. During a primary/backup switchover, the BFD session of the primary path might go down if a large number of MPLS TE tunnel interfaces exist, which results in traffic interruption. To resolve this issue, disable MPLS BFD from triggering tunnel-down. Then, the tunnel interface state remains unchanged when the BFD session of the MPLS TE tunnel interface goes down.
 - c. Return to system view.
quit
 4. Enter the view of an MPLS TE tunnel interface.
interface tunnel *number*
 5. (Optional.) Configure the capability of MPLS BFD to trigger tunnel-down.
mpls bfd trigger tunnel-down { **disable | **enable** }**
 By default, the configuration in MPLS TE view is used.

Command reference

mpls bfd trigger tunnel-down

Use **mpls bfd trigger tunnel-down** to configure the capability of MPLS BFD to trigger tunnel-down.

Use **undo mpls bfd trigger tunnel-down** to restore the default.

Syntax

mpls bfd trigger tunnel-down { **disable | **enable** }**
undo mpls bfd trigger tunnel-down { **disable | **enable** }**

Default

The configuration in MPLS TE view is used.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

disable: Disables MPLS BFD from triggering tunnel-down.

enable: Enables MPLS BFD to trigger tunnel-down.

Usage guidelines

If you configure static MPLS BFD in a primary/backup scenario, the device creates a BFD session for only the primary path. During a primary/backup switchover, the BFD session of the primary path might go down if a large number of MPLS TE tunnel interfaces exist, which results in traffic interruption. To resolve this issue, execute the **mpls bfd trigger tunnel-down disable** command to disable MPLS BFD from triggering tunnel-down. Then, the tunnel interface state remains unchanged when the BFD session of the MPLS TE tunnel interface goes down.

As a best practice, execute the **mpls tunnel-bfd** command to enable tunnel BFD on an MPLS TE tunnel interface after you disable MPLS BFD from triggering tunnel-down on the interface.

You can execute the **mpls bfd trigger tunnel-down** command in both MPLS TE view and MPLS TE tunnel interface view. The configuration in MPLS TE view takes effect on all MPLS TE tunnel interfaces. The configuration in MPLS TE tunnel interface view takes effect on only the current MPLS TE tunnel interface. For an MPLS TE tunnel interface, the configuration in MPLS TE tunnel interface view takes precedence over the configuration in MPLS TE view.

Examples

Enable MPLS BFD to trigger tunnel-down on interface Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode mpls-te
[Sysname-Tunnel1] mpls bfd trigger tunnel-down enable
```

Related commands

mpls bfd trigger tunnel-down enable

mpls bfd trigger tunnel-down enable

Use **mpls bfd trigger tunnel-down enable** to enable MPLS BFD to trigger tunnel-down.

Use **undo mpls bfd trigger tunnel-down enable** to disable MPLS BFD from triggering tunnel-down.

Syntax

mpls bfd trigger tunnel-down enable

undo mpls bfd trigger tunnel-down enable

Default

MPLS BFD is able to trigger tunnel-down. An MPLS TE tunnel interface goes down when its BFD session goes down.

Views

MPLS TE view

Predefined user roles

network-admin

Usage guidelines

If you configure static MPLS BFD in a primary/backup scenario, the device creates a BFD session for only the primary path. During a primary/backup switchover, the BFD session of the primary path might go down if a large number of MPLS TE tunnel interfaces exist, which results in traffic interruption. To resolve this issue, execute the **undo mpls bfd trigger tunnel-down enable** command to disable MPLS BFD from triggering tunnel-down. Then, the tunnel interface state remains unchanged when the BFD session of the MPLS TE tunnel interface goes down.

As a best practice, execute the **mpls tunnel-bfd** command to enable tunnel BFD on an MPLS TE tunnel interface after you disable MPLS BFD from triggering tunnel-down on the interface.

You can execute the **mpls bfd trigger tunnel-down enable** command in both MPLS TE view and MPLS TE tunnel interface view. The configuration in MPLS TE view takes effect on all MPLS TE tunnel interfaces. The configuration in MPLS TE tunnel interface view takes effect on only the current MPLS TE tunnel interface. For an MPLS TE tunnel interface, the configuration in MPLS TE tunnel interface view takes precedence over the configuration in MPLS TE view.

Examples

```
# Enable MPLS BFD to trigger tunnel-down.
<Sysname> system-view
[Sysname] mpls te
[Sysname-te] mpls bfd trigger tunnel-down enable
```

Related commands

mpls bfd trigger tunnel-down

New feature: Configuring resource monitoring

Configuring resource monitoring

About this task

The resource monitoring feature enables the device to monitor the available amounts of types of resources, for example, the space for ARP entries. The device samples the available amounts periodically and compares the samples with resource depletion thresholds to identify the resource depletion status.

The device supports a minor resource depletion threshold and a severe resource depletion threshold for each supported resource type.

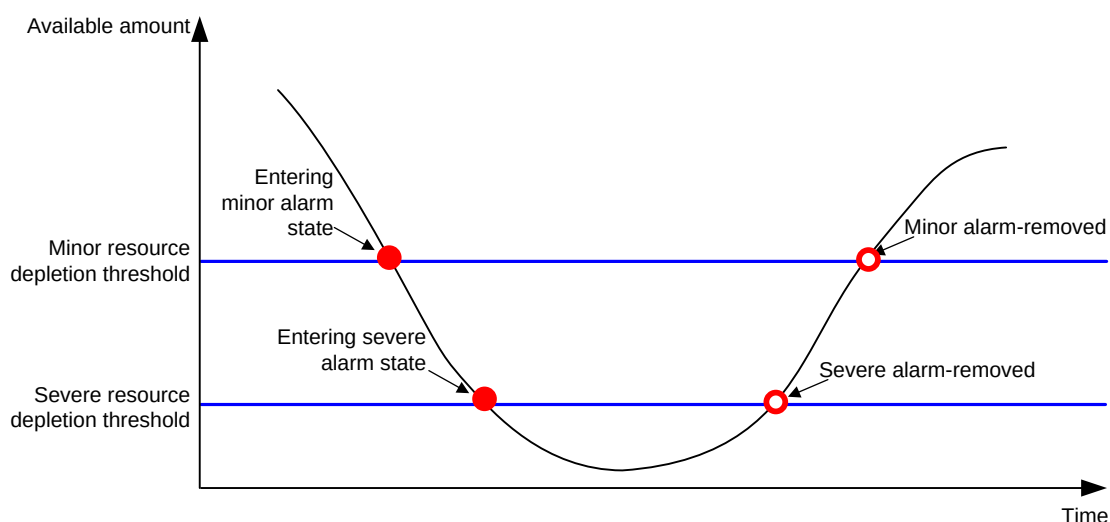
- If the available amount is equal to or less than the minor resource depletion threshold but greater than the severe resource depletion threshold, the resource type is in minor alarm state.
- If the available amount is equal to or less than the severe resource depletion threshold, the resource type is in severe alarm state.
- If the available amount increases above the minor resource depletion threshold, the resource type is in recovered state.

When a resource type enters severe alarm state, the device issues a severe alarm. If the resource type stays in severe alarm state, the device resends severe alarms periodically.

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

Resource depletion alarms can be sent to NETCONF, SNMP, and the information center to be encapsulated as NETCONF events, SNMP traps and informs, and log messages. For more information, see NETCONF, SNMP, and information center in *Network Management and Monitoring Configuration Guide*.

Figure 2 Resource depletion alarms and alarm-removed notifications



Hardware and feature compatibility

Hardware	Feature compatibility
MSR610	Yes
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	Yes
MSR1004S-5G	Yes
MSR1104S-W, MSR1104S-W-CAT	Yes
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	Yes
MSR 2630	Yes
MSR3600-28, MSR3600-51	Yes
MSR3600-28-SI, MSR3600-51-SI	Yes
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	Yes
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	Yes
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR 3610, MSR 3620, MSR 3620-DP, MSR 3640,	Yes

MSR 3660	
MSR3610-G, MSR3620-G	Yes
MSR3640-X1-HI	Yes

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	Yes
MSR2630-WiNet	Yes
MSR3600-28-WiNet	Yes
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	Feature compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	Yes
MSR2630-XS	Yes
MSR3600-28-XS	Yes
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	Yes
MSR3610-IE-XS	Yes
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Feature compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	Yes

Procedure

1. Enter system view.

system-view

2. Set resource depletion thresholds.

In standalone mode:

resource-monitor resource *resource-name* **cpu** *cpu-number* { **by-absolute** | **by-percent** } **minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

In IRF mode:

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* { **by-absolute** | **by-percent** } **minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

The default settings vary by resource type. Use the **display resource-monitor** command to display the resource depletion thresholds.

3. Specify destinations for resource depletion alarms.

resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

By default, resource depletion alarms are not sent to NETCONF, SNMP, or the information center.

4. Enable resending of minor resource depletion alarms.

resource-monitor minor resend enable

By default, resending of minor resource depletion alarms is enabled.

Command reference

display resource-monitor

Use **display resource-monitor** to display resource monitoring information.

Syntax

In standalone mode:

display resource-monitor [**resource** *resource-name*] [**cpu** *cpu-number*]

In IRF mode:

display resource-monitor [**resource** *resource-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	Yes
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No

Hardware	Command compatibility
MSR810-LMS-EA, MSR810-LME	Yes
MSR1004S-5G	Yes
MSR1104S-W, MSR1104S-W-CAT	Yes
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	Yes
MSR 2630	Yes
MSR3600-28, MSR3600-51	Yes
MSR3600-28-SI, MSR3600-51-SI	Yes
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	Yes
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	Yes
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR 3610, MSR 3620, MSR 3620-DP, MSR 3640, MSR 3660	Yes
MSR3610-G, MSR3620-G	Yes
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	Yes
MSR2630-WiNet	Yes
MSR3600-28-WiNet	Yes
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	Command compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	Yes

Hardware	Command compatibility
MSR2630-XS	Yes
MSR3600-28-XS	Yes
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	Yes
MSR3610-IE-XS	Yes
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	Yes

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

resource *resource-name*: Specifies a resource type by its name. See [Table 37](#) for the resource types.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays resource monitoring information for all member devices. (In IRF mode.)

cpu *cpu-number*: Specifies a CPU by its number.

Examples

(In standalone mode.) Display IPv4 FIB resource monitoring information.

```
<Sysname> display resource-monitor resource ipv4fib
```

```
Minor alarms resending: Enabled
```

```
Resource
```

```
Minor Severe Free/Total
```

```

                                (absolute)
ipv4fib                        20%   10%   19990/20000

# (In IRF mode.) Display IPv4 FIB resource monitoring information.
<Sysname> display resource-monitor resource ipv4fib
Minor alarms resending: Enabled

Slot 1:
Resource                        Minor Severe Free/Total
                                (absolute)
ipv4fib                        20%   10%   19990/20000

```

Table 36 Command output

Field	Description
Minor alarms resending	Status of the minor resource depletion alarm resending feature: • Enabled. • Disabled.
Resource	Monitored resource type.
Minor (%)	Minor resource depletion threshold, in percentage.
Severe (%)	Severe resource depletion threshold, in percentage.
Free/Total (absolute)	Numbers of available resources and total resources, in absolute values.

Related commands

resource-monitor minor resend enable

resource-monitor resource

resource-monitor minor resend enable

Use **resource-monitor minor resend enable** to enable resending of minor resource depletion alarms.

Use **undo resource-monitor minor resend enable** to disable resending of minor resource depletion alarms.

Syntax

resource-monitor minor resend enable

undo resource-monitor minor resend enable

Default

Resending of minor resource depletion alarms is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

The resending period is fixed at 24 hours for a severe alarm and is fixed at 7 * 24 hours for a minor alarm.

Examples

```
# Enable resending of minor resource depletion alarms.
<Sysname> system-view
[Sysname] resource-monitor minor resend enable
```

Related commands

display resource-monitor

resource-monitor output

resource-monitor resource

resource-monitor output

Use **resource-monitor output** to specify destinations for resource depletion alarms.

Use **undo resource-monitor output** to remove destinations for resource depletion alarms.

Syntax

resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

undo resource-monitor output [**netconf-event** | **snmp-notification** | **syslog**] *

Default

Resource depletion alarms are not sent to NETCONF, SNMP, or the information center.

Views

System view

Predefined user roles

network-admin

Parameters

netconf-event: Sends resource depletion alarms to the NETCONF feature to encapsulate the alarms in NETCONF events. For more information, see NETCONF in *Network Management and Monitoring Configuration Guide*.

snmp-notification: Sends resource depletion alarms to the SNMP feature to encapsulate the alarms in SNMP traps and informs. For more information, see SNMP in *Network Management and Monitoring Configuration Guide*.

syslog: Sends resource depletion alarms to the information center to encapsulate the alarms in log messages. For more information, see information center in *Network Management and Monitoring Configuration Guide*.

Usage guidelines

If you do not specify any keywords for the **undo resource-monitor output** command, the command disables resource depletion alarm output.

Examples

Specify the information center module as the output destination for resource depletion alarms.

```
<Sysname> system-view
```

```
[Sysname] resource-monitor output syslog
```

Related commands

resource-monitor minor resend enable

resource-monitor resource

resource-monitor resource

Use **resource-monitor resource** to set resource depletion thresholds.

Use **undo resource-monitor resource** to disable resource depletion thresholds.

Syntax

In standalone mode:

resource-monitor resource *resource-name* **cpu** *cpu-number* { **by-absolute** | **by-percent** } **minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **cpu** *cpu-number*

In IRF mode:

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* { **by-absolute** | **by-percent** } **minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number*

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	Yes
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	Yes
MSR1004S-5G	Yes
MSR1104S-W, MSR1104S-W-CAT	Yes
MSR2600-6-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	Yes
MSR 2630	Yes
MSR3600-28, MSR3600-51	Yes
MSR3600-28-SI, MSR3600-51-SI	Yes
MSR3600-28-X1, MSR3600-28-X1-DP,	Yes

Hardware	Command compati bility
MSR3600-51-X1, MSR3600-51-X1-DP	
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	Yes
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR 3610, MSR 3620, MSR 3620-DP, MSR 3640, MSR 3660	Yes
MSR3610-G, MSR3620-G	Yes
MSR3640-X1-HI	Yes

Hardware	Command compati bility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	Yes
MSR2630-WiNet	Yes
MSR3600-28-WiNet	Yes
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	Command compati bility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	Yes
MSR2630-XS	Yes
MSR3600-28-XS	Yes
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	Yes
MSR3610-IE-XS	Yes
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	Yes

Default

The default settings vary by resource type. Use the **display resource-monitor** command to display the resource depletion thresholds.

Views

System view

Predefined user roles

network-admin

Parameters

resource-name: Specifies a resource type by its name. The values for this argument are case insensitive and cannot be abbreviated. [Table 37](#) shows the resource types that can be monitored.

Table 37 Resource types that can be monitored

Resource type	Description
acl_rule	ACL resources.
ipv4fib	IPv4 FIB table resources.
ipv6fib	IPv6 FIB table resources.

slot slot-number: Specifies an IRF member device by its member ID. (In IRF mode)

cpu cpu-number: Specifies a CPU by its number.

by-absolute: Specifies resource depletion thresholds by using absolute values.

by-percent: Specifies resource depletion thresholds in percentage.

minor-threshold minor-threshold: Specifies the minor resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *minor-threshold* argument.

severe-threshold severe-threshold: Specifies the severe resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *severe-threshold* argument.

Usage guidelines

After you execute this command for a resource type, the device monitors the available amount of the type of resources. The device samples the available amount at intervals, compares the sample with the resource depletion thresholds to identify the resource depletion status, and sends alarms as configured.

Examples

(In standalone mode.) Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for IPv4 FIB resources.

```
<Sysname> system-view
```

```
[Sysname] resource-monitor resource ipv4fib cpu 0 by-percent minor-threshold 30  
severe-threshold 10
```

(In IRF mode.) Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for IPv4 FIB resources.

```
<Sysname> system-view
```

```
[Sysname] resource-monitor resource ipv4fib slot 1 cpu 0 by-percent minor-threshold 30  
severe-threshold 10
```

Related commands

display resource-monitor

resource-monitor minor resend enable

resource-monitor output

New feature: Tunnel BFD for LSPs

Configuring tunnel BFD for LSPs

About this task

The **mpls bfd** command can detect only the primary LSP failure. When the primary LSP fails, BFD can quickly detect the failure and notify the device to switch traffic to the backup LSP. When both the primary and backup LSPs fail, the BFD detection mechanism fails. Traffic is lost until another mechanism detects the failures and triggers a traffic protection measure (such as MPLS L3VPN ECMP route based load balancing and FRR).

To resolve this issue, you can execute the **mpls tunnel-bfd** command to configure tunnel BFD, which detects failures on the primary LSP and all the backup LSPs. When both the primary LSP and current backup LSP fail, tunnel BFD can quickly detect the failures and trigger a traffic protection measure to switch traffic to an available backup LSP.

Restrictions and guidelines

To configure tunnel BFD for an LSP, configure both the local and remote devices as described in [Table 38](#).

Table 38 Configurations on the local and remote devices

BFD session establishment mode	Node type	Execute the "mpls bfd enable" command?	Execute the "mpls tunnel-bfd" command?	Configure the discriminator keyword?
Static mode	Local	Yes	Yes	Yes
	Remote	Yes	Yes	Yes
Dynamic mode	Local	Yes	Yes	No
	Remote	Yes	No	N/A

Follow these guidelines to configure tunnel BFD for an LSP tunnel:

- To establish a static BFD session, ensure that the local and remote discriminators configured locally are identical with the remote and local discriminators configured on the remote device, respectively.
- On a BFD session established in static mode, the ingress node and egress node both operate in active mode. On a BFD session established in dynamic mode, the ingress node operates in passive mode and the egress node operates in active mode. Executing the **bfd session init-mode** command on the ingress or egress node does not change the node's operating mode.

Prerequisites

The source address of the BFD session is the MPLS LSR ID of the local device. Before configuring tunnel BFD for the LSP tunnel, perform the following tasks:

- Configure an MPLS LSR ID for the local device.
- Make sure a route is available on the remote device to reach the MPLS LSR ID.

Configuring control packet mode tunnel BFD for LSPs

1. Enter system view.

system-view

2. Enable BFD for MPLS.

mpls bfd enable

By default, BFD for MPLS is disabled.

3. (Optional.) Remove the Router Alert option in BFD packets.

undo bfd ip-router-alert

By default, the Router Alert option is carried in BFD packets for LSP connectivity verification.

Execute this command on the local device if the peer device cannot identify the Router Alert option in BFD packets.

This command takes effect only on BFD sessions that come up after this command is executed.

4. Configure control packet mode tunnel BFD to verify LSP connectivity for an FEC.

- To use a static BFD session:

mpls tunnel-bfd *dest-addr mask-length discriminator local local-id remote remote-id* [**bgp-lsp** | **isis-srlsp** | **ldp-lsp** | **ospf-srlsp** | **static-lsp**] [**template** *template-name*]

- To use a dynamic BFD session:

mpls tunnel-bfd *dest-addr mask-length* [**ldp-fec** | **nil-fec**] [**template** *template-name*]

By default, tunnel BFD is not configured to verify LSP connectivity for an FEC.

Configuring echo packet mode tunnel BFD for LSPs

1. Enter system view.

system-view

2. Enable BFD for MPLS.

mpls bfd enable

By default, BFD for MPLS is disabled.

3. (Optional.) Remove the Router Alert option in BFD packets.

undo bfd ip-router-alert

By default, the Router Alert option is carried in BFD packets for LSP connectivity verification.

Execute this command on the local device if the peer device cannot identify the Router Alert option in BFD packets.

This command takes effect only on BFD sessions that come up after this command is executed.

4. Configure echo packet mode tunnel BFD to verify LSP connectivity for an FEC.

mpls tunnel-bfd *dest-addr mask-length* **echo** [**template** *template-name*]

By default, tunnel BFD is not configured to verify LSP connectivity for an FEC.

Command reference

mpls tunnel-bfd (for LSP)

Use **mpls tunnel-bfd** to enable tunnel BFD for LSPs associated with an FEC.

Use **undo mpls tunnel-bfd** to disable tunnel BFD for LSPs associated with an FEC.

Syntax

mpls tunnel-bfd *dest-addr mask-length* [**discriminator** **local** *local-id* **remote** *remote-id* [**bgp-lsp** | **isis-srlsp** | **ldp-lsp** | **ospf-srlsp** | **static-lsp**] | **echo** | **ldp-fec** | **nil-fec**] [**template** *template-name*]

undo mpls tunnel-bfd *dest-addr mask-length*

Default

Tunnel BFD is not used to verify LSP connectivity for an FEC.

Views

System view

Predefined user roles

network-admin

Parameters

dest-addr mask-length: Specifies an FEC by a destination IP address and mask length. The mask length is in the range of 0 to 32.

discriminator: Specifies discriminator values for the BFD session.

local local-id: Specifies the local discriminator value for the BFD session. The value range is 1 to 32768.

remote remote-id: Specifies the remote discriminator value for the BFD session, in the range of 1 to 4294967295.

bgp-lsp: Specifies BGP LSP.

isis-srlsp: Specifies IS-IS SRLSP.

ldp-lsp: Specifies LDP LSP.

ospf-srlsp: Specifies OSPF SRLSP.

static-lsp: Specifies static LSP.

echo: Specifies the BFD echo packet mode. If you do not specify this keyword, the BFD control packet mode is used to verify LSP connectivity.

ldp-fec: Encapsulates the LDP IPv4 Prefix FEC in MPLS echo request packets when BFD control packet mode is used to detect LSPs. If you do not specify this keyword, the type of the FEC carried in MPLS echo request packets is IPv4 IGP-Prefix Segment ID. The egress node of an LSP might

support only the LDP IPv4 Prefix FEC. If the ingress node sends MPLS echo request packets that carry the IPv4 IGP-Prefix Segment ID type of FEC, the egress node cannot recognize this FEC type. The FEC validation on the egress node will fail and the BFD session will go down. To resolve this issue, specify the **ldp-fec** keyword to enable the ingress node to encapsulate the LDP IPv4 Prefix FEC in MPLS echo request packets. Then, FEC validation on the egress node can be successful.

nil-fec: Encapsulates the Nil FEC in MPLS echo request packets when BFD control packet mode is used to detect LSPs. In LDP to SR interworking mode, the ingress node (source node) cannot determine whether the LDP LSP is connected to the SRLSP. When the ingress node uses MPLS BFD to detect LSPs, it encapsulates LDP FEC in MPLS echo request packets, which will fail the FEC type verification on the egress node (end-point node). Then, the BFD session will go down. To resolve this issue, specify the **nil-fec** keyword to enable the ingress node to encapsulate the Nil FEC in MPLS echo request packets. The egress node will not check the FEC type of packets encapsulated with the Nil FEC.

template *template-name*: Specifies a BFD session parameter template by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a template, BFD control packet mode uses the multihop BFD session settings configured in system view, and BFD echo packet mode uses the system default BFD session settings.

Usage guidelines

The **mpls bfd** command can detect only the primary LSP failure. When the primary LSP fails, BFD can quickly detect the failure and notify the device to switch traffic to the backup LSP. When both the primary and backup LSPs fail, the BFD detection mechanism fails. Traffic is lost until another mechanism detects the failures and triggers a traffic protection measure (such as MPLS L3VPN ECMP route based load balancing and FRR) to take effect.

To resolve this issue, you can execute the **mpls tunnel-bfd** command to configure tunnel BFD, which detects failures on the primary LSP and all the backup LSPs. When both the primary LSP and current backup LSP fail, tunnel BFD can quickly detect the failures and trigger a traffic protection measure to switch traffic to an available backup LSP.

The source address of the BFD session is the MPLS LSR ID of the local device. Before configuring tunnel BFD for LSPs, perform the following tasks:

- Configure an MPLS LSR ID for the local device.
- Make sure a route is available on the remote device to reach the MPLS LSR ID.

When BFD control packet mode is used to verify LSP connectivity, a BFD session can be established in one of the following modes:

- **Static mode**—Specify the local and remote discriminator values by using the **discriminator** keyword in the **mpls tunnel-bfd** command. You must enable BFD for MPLS and execute the **mpls tunnel-bfd** command on both the local and remote devices. Make sure the discriminators configured on the local device match those configured on the remote device. A static BFD session verifies connectivity of a pair of LSPs in opposite directions between two devices.
- **Dynamic mode**—If you do not specify local and remote discriminators, the system automatically runs MPLS ping to negotiate the discriminator values. You must enable BFD for MPLS on both the local and remote devices, but the **mpls tunnel-bfd** command is not needed on the remote device. A dynamic BFD session verifies the connectivity of a unidirectional LSP from the local device to the remote device.

To enable the BFD echo packet mode, you must first execute the **bfd echo-source-ip** command on the local device to specify a source IP address for BFD echo packets.

If you do not specify the **bgp-lsp**, **isis-srlsp**, **ldp-lsp**, **ospf-srlsp**, or **static-lsp** keyword when executing the **mpls tunnel-bfd** command, BFD detects the LSPs in the following sequence:

1. Static LSP.
2. LDP LSP.
3. BGP LSP.
4. OSPF SRLSP.

5. IS-IS SRLSP.

The BFD session is up as long as one LSP is operating correctly. The BFD session goes down when all LSPs fail.

Examples

```
# Use tunnel BFD to verify the connectivity of the LSPs to destination 22.22.2.2/32.
```

```
<Sysname> system-view
```

```
[Sysname] mpls bfd enable
```

```
[Sysname] mpls bfd 22.22.2.2 32
```

Related commands

display mpls bfd

mpls bfd enable

New feature: Tunnel BFD for MPLSTE tunnels

Configuring tunnel BFD for MPLS TE tunnels

About this task

In an MPLS TE CRLSP backup scenario, you can use the **mpls bfd** command to create a BFD session for the primary and backup CRLSPs, respectively. When the primary CRLSP fails, BFD can quickly detect the failure and notify the device to switch traffic to the backup CRLSP. When both the primary and backup CRLSPs fail, the BFD detection mechanism fails. Traffic is lost until another mechanism detects the failure and triggers a traffic protection measure (such as MPLS L3VPN ECMP route based load balancing and FRR) to take effect.

To resolve this issue, you can execute the **mpls tunnel-bfd** command to configure tunnel BFD, which detects failures on the primary CRLSP and all the backup CRLSPs. When both the primary CRLSP and the current backup CRLSP fail, tunnel BFD can quickly detect the failures and trigger a traffic protection measure to switch traffic to an available backup CRLSP.

Restrictions and guidelines

To run tunnel BFD on an MPLS TE tunnel, configure both the local and remote devices as described in [Table 39](#).

Table 39 Configurations on the local and remote devices

BFD session establishment mode	Node type	Execute the "mpls bfd enable" command?	Execute the "mpls tunnel-bfd" command?	Configure the discriminat or keyword?
Static mode	Local	Yes	Yes	Yes
	Remote	Yes	Yes	Yes
Dynamic mode	Local	Yes	Yes	No
	Remote	Yes	No	N/A

Follow these guidelines to configure tunnel BFD for an MPLS TE tunnel:

- To establish a static BFD session, ensure that the local and remote discriminators configured locally are identical with the remote and local discriminators configured on the remote device, respectively.

- On a BFD session established in static mode, the ingress node and egress node both operate in active mode. On a BFD session established in dynamic mode, the ingress node operates in passive mode and the egress node operates in active mode. Executing the **bfd session init-mode** command on the ingress or egress node does not change the node's operating mode.

After you configure tunnel BFD for an MPLS TE tunnel, use one of the following commands to disable MPLS BFD from triggering tunnel-down to avoid tunnel flapping:

- mpls bfd trigger tunnel-down disable** (in tunnel interface view)
- undo mpls bfd trigger tunnel-down enable** (in MPLS TE view)

Prerequisites

The source address of the BFD session is the MPLS LSR ID of the local device. Before configuring BFD for the LSP tunnel, perform the following tasks:

- Configure an MPLS LSR ID for the local device.
- Make sure a route is available on the remote device to reach the MPLS LSR ID.

To enable the BFD echo packet mode, you must first configure the **bfd echo-source-ip** command on the local device to specify a source IP address for BFD echo packets.

Configuring control packet mode tunnel BFD for an MPLS TE tunnel

- Enter system view.
system-view
- Enable BFD for MPLS.
mpls bfd enable
By default, BFD for MPLS is disabled.
- (Optional.) Enable dynamic establishment of passive mode BFD sessions.
mpls bfd passive enable
By default, device can dynamically establish passive mode BFD sessions.
This command is required only on the egress node to establish a dynamic BFD session.
- Enter the view of an MPLS TE tunnel interface.

- Configure control packet mode tunnel BFD to verify MPLS TE tunnel connectivity.
 - To use a static BFD session:
mpls tunnel-bfd discriminator local *local-id* remote *remote-id* [template *template-name*]
 - To use a dynamic BFD session:
mpls tunnel-bfd [template *template-name*]

By default, tunnel BFD is not configured to verify MPLS TE tunnel connectivity.

If you specify templates for both BFD and tunnel BFD, specify greater interval settings for the BFD template than the tunnel BFD template. This rule ensures that the tunnel BFD session for MPLS TE tunnel is up after a primary/backup LSP switchover.

Configuring echo packet mode tunnel BFD for an MPLS TE tunnel

- Enter system view.
system-view
- Enable BFD for MPLS.
mpls bfd enable
By default, BFD for MPLS is disabled.

3. (Optional.) Enable dynamic establishment of passive mode BFD sessions.
mpls bfd passive enable
 By default, device can dynamically establish passive mode BFD sessions.
 This command is required only on the egress node to establish a dynamic BFD session.
4. Enter the view of an MPLS TE tunnel interface.
interface tunnel *number*
5. Configure echo packet mode tunnel BFD to verify MPLS TE tunnel connectivity.
mpls tunnel-bfd echo [**template *template-name*]**
 By default, tunnel BFD is not configured to verify MPLS TE tunnel connectivity.
 If you specify templates for both BFD and tunnel BFD, specify greater interval settings for the BFD template than the tunnel BFD template. This rule ensures that the tunnel BFD session for MPLS TE tunnel is up after a primary/backup LSP switchover.

Command reference

mpls tunnel-bfd (for TE tunnel)

Use **mpls tunnel-bfd** to enable tunnel BFD on an MPLS TE tunnel interface.

Use **undo mpls tunnel-bfd** to restore the default.

Syntax

mpls tunnel-bfd [**discriminator **local** *local-id* **remote** *remote-id* | **echo**] [**template** *template-name*]**

undo mpls tunnel-bfd

Default

Tunnel BFD is not used to verify MPLS TE tunnel connectivity on a tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

discriminator: Specifies discriminator values for the BFD session.

local *local-id*: Specifies the local discriminator value for the BFD session, in the range of 1 to 32768.

remote *remote-id*: Specifies the remote discriminator value for the BFD session, in the range of 1 to 4294967295.

echo: Enables the BFD echo packet mode.

template *template-name*: Specifies a BFD session parameter template by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a template, BFD control packet mode uses the multihop BFD session settings configured in system view, and BFD echo packet mode uses the system default BFD session settings.

Usage guidelines

In an MPLS TE CRLSP backup scenario, you can use the **mpls bfd** command to create a BFD session for the primary and backup CRLSPs, respectively. When the primary CRLSP fails, BFD can quickly detect the failure and notify the device to switch traffic to the backup CRLSP. When both the

primary and backup CRLSPs fail, the BFD detection mechanism fails. Traffic is lost until another mechanism detects the failure and triggers a traffic protection measure (such as MPLS L3VPN ECMP route based load balancing and FRR) to take effect.

To resolve this issue, you can execute the **mpls tunnel-bfd** command to configure tunnel BFD, which detects failures on the primary CRLSP and all the backup CRLSPs. When both the primary CRLSP and the current backup CRLSP fail, tunnel BFD can quickly detect the failures and trigger a traffic protection measure to switch traffic to an available backup CRLSP.

The source address of the BFD session is the MPLS LSR ID of the local device. Before configuring tunnel BFD for an MPLS TE tunnel, perform the following tasks:

- Configure an MPLS LSR ID for the local device.
- Make sure a route is available on the remote device to reach the MPLS LSR ID.

If you do not specify the **echo** keyword, this command enables the BFD control packet mode to verify the MPLS TE tunnel connectivity.

When BFD control packet mode is used, a BFD session can be established in one of the following modes:

- **Static mode**—Specify the local and remote discriminators by using the **discriminator** keyword in the **mpls tunnel-bfd** command. You must execute the **mpls bfd enable** and **mpls tunnel-bfd** commands on both the local and remote devices. Make sure the local discriminator and remote discriminator on the local device are the same as the remote discriminator and local discriminator on the remote device, respectively. A static BFD session verifies the connectivity of a pair of MPLS TE tunnels in opposite directions between two devices.
- **Dynamic mode**—If you do not specify local and remote discriminators, the system automatically runs MPLS ping to negotiate the discriminator values. You must execute the **mpls bfd enable** command on both the local and remote devices, but the **mpls tunnel-bfd** command is not needed on the remote device. A dynamic BFD session verifies the connectivity of a unidirectional MPLS TE tunnel from the local device to the remote device.

To enable the BFD echo packet mode, you must first execute the **bfd echo-source-ip** command on the local device to specify a source IP address for BFD echo packets.

After you configure the **mpls tunnel-bfd** command for a tunnel, use one of the following commands to disable MPLS BFD from triggering tunnel-down to avoid tunnel flapping:

- **mpls bfd trigger tunnel-down disable** (in tunnel interface view)
- **undo mpls bfd trigger tunnel-down enable** (in MPLS TE view)

Examples

Enable tunnel BFD to verify tunnel connectivity on MPLS TE tunnel interface **Tunnel 1**, and use the BFD session parameter template **test**.

```
<Sysname> system-view
[Sysname] mpls bfd enable
[Sysname] interface tunnel 1 mode mpls-te
[Sysname-Tunnel1] mpls tunnel-bfd template test
```

Related commands

display mpls bfd
mpls bfd enable

New feature: Configuring the rule for adding BGP routes to the IP routing table

and the route advertisement rule for VPN instances

Configuring the rule for adding BGP routes to the IP routing table and the route advertisement rule for VPN instances

About this task

Perform this task to configure the following features:

- For routes to the same destination address, BGP adds the optimal route with the same route targets as a VPN instance to the IP routing table of the VPN instance.

After you execute the **undo policy vpn-target** command, a VPNv4 route that has different route targets than a VPN instance can be added to the BGP routing table of the VPN instance, and the route can be selected as the optimal route. However, the route cannot be added to the IP routing table of the VPN instance, making the route unreachable in the VPN instance.

You can configure this feature to resolve this issue. With this feature configured, for BGP routes to the same destination address, BGP adds the optimal route with the same route targets as a VPN instance to the IP routing table of the VPN instance.

For example, the import target of VPN instance **vpna** is 10:1. The BGP routing table of VPN instance **vpna** contains two routes to destination address 1.1.1.1, which are 1.1.1.1 <RT: 10:1> and 1.1.1.1 <RT: 20:1>, and 1.1.1.1 <RT: 20:1> is the optimal route. After you configure this feature, BGP will add 1.1.1.1 <RT: 10:1> to the IP routing table of VPN instance **vpna**, because this route has the same import target as the VPN instance.

- When the optimal route to a destination address cannot be advertised to peers, the device advertises the route with the highest priority to the destination address from the routes that can be advertised. The device does not advertise any route for a destination address if no routes to the destination address can be advertised.

The BGP routing table of a VPN instance contains the routes in the IP routing table of the VPN instance, so the routing table of a BGP address family might contain routes that are not learned from the address family. For example, an IP prefix route learned from the BGP EVPN address family is added to the IP routing table of a VPN instance, and the route also exists in the BGP routing tables of the BGP-VPN IPv4 unicast address family and BGP VPNv4 address family in the VPN instance. BGP cannot advertise the optimal route to peers in an address family if the optimal route is not learned from the address family, making the destination address of the route unreachable.

After you configure this feature, if the optimal route to a destination address cannot be advertised to peers, the device advertises the route with the highest priority to the destination address from the routes that can be advertised. The device does not advertise any route for a destination address if no routes to the destination address can be advertised.

For example, the device learns the route with IP prefix 3.3.3.3/32 from both the BGP VPNv4 address family and BGP EVPN address family. Therefore, there will be two routes to destination address 3.3.3.3 in the BGP routing table of the BGP VPNv4 address family, and the one learned from the BGP EVPN address family is the optimal route. However, this optimal route cannot be advertised to BGP VPNv4 peers, because it was learned from the BGP EVPN address family. As a result, network nodes deployed with only BGP VPNv4 cannot obtain the route with IP prefix 3.3.3.3/32. After you configure this feature, the device will advertise the route with IP prefix 3.3.3.3/32 learned from the BGP VPNv4 address family to BGP VPNv4 peers, although this route is not the optimal route.

Restrictions and guidelines

The **bestroute same-rd** command takes effect on BGP routes of all VPN instances. Use caution when you execute this command.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Configure BGP to add the optimal routes with the same route targets as a VPN instance to the IP routing table of the VPN instance, and allow BGP to advertise non-optimal routes to its peers.

bestroute same-rd

By default, BGP adds the optimal routes in the BGP routing table to the IP routing table of a VPN instance and advertises only the optimal routes to its peers.

Command reference

New command: **bestroute same-rd**

Use **bestroute same-rd** to configure BGP to add the optimal routes with the same route targets as a VPN instance to the IP routing table of the VPN instance and allow BGP to advertise non-optimal routes to its peers.

Use **undo bestroute same-rd** to restore the default.

Syntax

bestroute same-rd

undo bestroute same-rd

Default

BGP adds the optimal routes in the BGP routing table to the IP routing table of a VPN instance and advertises only the optimal routes to its peers.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines



IMPORTANT:

This command takes effect on BGP routes of all VPN instances.
Use caution when you execute this command.

Execute this command to configure the following features:

- For routes to the same destination address, BGP adds the optimal route with the same route targets as a VPN instance to the IP routing table of the VPN instance.

After you execute the **undo policy vpn-target** command, a VPNv4 or VPNv6 route that has different route targets than a VPN instance can be added to the BGP routing table of the VPN instance, and the route can be selected as the optimal route. However, the route cannot be

added to the IP routing table of the VPN instance, making the route unreachable in the VPN instance.

You can execute this command to resolve this issue. With this command configured, for BGP routes to the same destination address, BGP adds the optimal route with the same route targets as a VPN instance to the IP routing table of the VPN instance.

For example, the import target of VPN instance **vpna** is 10:1. The BGP routing table of VPN instance **vpna** contains two routes to destination address 1.1.1.1, which are 1.1.1.1 <RT: 10:1> and 1.1.1.1 <RT: 20:1>, and 1.1.1.1 <RT: 20:1> is the optimal route. After you execute this command, BGP will add 1.1.1.1 <RT: 10:1> to the IP routing table of VPN instance **vpna**, because this route has the same import target as the VPN instance.

- When the optimal route to a destination address cannot be advertised to peers, the device advertises the route with the highest priority to the destination address from the routes that can be advertised. The device does not advertise any route for a destination address if no routes to the destination address can be advertised.

The BGP routing table of a VPN instance contains the routes in the IP routing table of the VPN instance, so the routing table of a BGP address family might contain routes that are not learned from the address family. For example, an IP prefix route learned from the BGP EVPN address family is added to the IP routing table of a VPN instance, and the route also exists in the BGP routing tables of the BGP-VPN IPv4 unicast address family and BGP VPNv4 address family in the VPN instance. BGP cannot advertise the optimal route to peers in an address family if the optimal route is not learned from the address family, making the destination address of the route unreachable.

After you execute this command, if the optimal route to a destination address cannot be advertised to peers, the device advertises the route with the highest priority to the destination address from the routes that can be advertised. The device does not advertise any route for a destination address if no routes to the destination address can be advertised.

For example, the device learns the route with IP prefix 3.3.3.3/32 from both the BGP VPNv4 address family and BGP EVPN address family. Therefore, there will be two routes to destination address 3.3.3.3 in the BGP routing table of the BGP VPNv4 address family, and the one learned from the BGP EVPN address family is the optimal route. However, this optimal route cannot be advertised to BGP VPNv4 peers, because it was learned from the BGP EVPN address family. As a result, network nodes deployed with only BGP VPNv4 cannot obtain the route with IP prefix 3.3.3.3/32. After you execute this command, the device will advertise the route with IP prefix 3.3.3.3/32 learned from the BGP VPNv4 address family to BGP VPNv4 peers, although this route is not the optimal route.

Examples

In BGP instance view, configure BGP to add the optimal routes with the same route targets as a VPN instance to the IP routing table of the VPN instance and allow BGP to advertise non-optimal routes to its peers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bestroute same-rd
```

Related commands

display bgp routing-table vpnv4

display bgp routing-table vpnv6
policy vpn-target

Modified command: display bgp routing-table vpnv4

Syntax

display bgp [**instance** *instance-name*] **routing-table vpnv4** [**same-rd-selected**]

Views

Any view

Change description

The **same-rd-selected** keyword was added.

same-rd-selected: Displays only the routes that BGP adds to the VPN instance IPv4 routing table after the **bestroute same-rd** command is executed. If you do not specify this keyword, the command displays information about all BGP VPNv4 routes.

Modified command: **display bgp routing-table vpnv6**

Syntax

display bgp [**instance** *instance-name*] **routing-table vpnv6** [**same-rd-selected**]

Views

Any view

Change description

The **same-rd-selected** keyword was added.

same-rd-selected: Displays only the routes that BGP adds to the VPN instance IPv6 routing table after the **bestroute same-rd** command is executed. If you do not specify this keyword, the command displays information about all BGP VPNv6 routes.

New feature: Specifying an MPLS label allocation mode

Specifying an MPLS label allocation mode

1. Enter system view.
system-view
2. Create a VPN instance and enter VPN instance view.
ip vpn-instance *vpn-instance-name*
3. Configure an RD for the VPN instance.
route-distinguisher *route-distinguisher*
By default, no RD is configured for a VPN instance.
4. Enter VPN instance IPv4 address family view.
address-family ipv4
5. Specify a label allocation mode.
apply-label { **per-instance** [**static** *static-label-value*] | **per-route** }
By default, BGP allocates a label to each next hop.

CAUTION:

Executing this command will re-advertise all routes in the VPN instance, which will cause temporary interruption of running services in the VPN instance. Please be cautious.

Command reference

Use **apply-label** to specify a label allocation mode.

Use **undo apply-label** to restore the default.

Syntax

```
apply-label { per-instance [ static static-label-value ] | per-route }  
undo apply-label
```

Default

BGP allocates labels on a per-next-hop basis.

Views

VPN instance IPv4 address family view

VPN instance IPv6 address family view

Predefined user roles

network-admin

Parameters

per-instance: Allocates a label to each VPN instance. All routes in the VPN instance use the same label.

static static-label-value: Specifies a static label value in the range of 16 to 1048575. If you do not specify this option, BGP randomly allocates a label value to the VPN instance.

per-route: Allocates a label to each route. Each route in the VPN instance uses an exclusive label.

Usage guidelines



CAUTION:

After you change the label allocation mode, BGP re-advertises all routes in the VPN instance, which will cause service interruption. Use this command with caution.

BGP supports the following label allocation modes:

- **Per-next-hop**—Allocates a label to each next hop. Use this mode when the number of labels required by the per-route mode exceeds the maximum number of labels supported by the device.
- **Per-route**—Allocates a label to each route.
- **Per-VPN-instance**—Allocates a label to each VPN instance. Use this mode when a large number of VPN routes exist on the PE.

Examples

In VPN instance IPv4 address family view, allocate static label **10000** to VPN instance **vpn1**.

```
<Sysname> system-view  
[Sysname] ip vpn-instance vpn1  
[Sysname-vpn-instance-vpn1] address-family ipv4  
[Sysname-vpn-ipv4-vpn1] apply-label per-instance static 10000  
This configuration causes service interruption. Continue? [Y/N]:y
```

New feature: Setting an MPLS label range for all VPN instances

Setting an MPLS label range for all VPN instances

1. Enter system view.
system-view
2. Set an MPLS label range for all VPN instances.
mpls per-vrf-label range *minimum maximum*

Command reference

mpls per-vrf-label range

Use **mpls per-vrf-label range** to specify a label range for all VPN instances.

Use **undo mpls per-vrf-label range** to restore the default.

Syntax

mpls per-vrf-label range *minimum maximum*

undo mpls per-vrf-label range

Default

No label range is specified for VPN instances.

Views

System view

Predefined user roles

network-admin

Parameters

minimum: Specifies the minimum label value, in the range of 15000 to 1048574.

maximum: Specifies the maximum label value, in the range of 15001 to 1048575.

Usage guidelines

Configure this command to specify the range of labels that a PE can allocate to VPN instances.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the label range for all VPN instances to 100000 to 104095.

```
<Sysname> system-view
```

```
[Sysname] mpls per-vrf-label range 100000 104095
```

New feature: Applying the export routing policy to VPNv4 routes before RT filtering

Applying the export routing policy to VPNv4 routes before RT filtering

About this task

By default, a device performs RT filtering on VPNv4 routes and then applies the export routing policy to the matching routes before advertisement. In some networks, no route targets are configured in the VPN instance, and the route targets of VPNv4 routes are configured through the export routing policy. If IPv4 RT filter route exchange is enabled for the device and its peer, all VPNv4 routes cannot pass RT filtering, and no VPNv4 routes can be advertised.

To resolve this issue, you can perform this task to configure the device to apply the export routing policy to VPNv4 routes before RT filtering.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP IPv4 RT filter address family view.
address-family ipv4 rtfilter
4. Apply the export routing policy to VPNv4 routes before RT filtering.
rtfilter check-after-policy

By default, a device performs RT filtering on VPNv4 routes and then applies the export routing policy to the matching routes before advertisement.

Command reference

rtfilter check-after-policy

Use **rtfilter check-after-policy** to apply the export routing policy to VPNv4 routes before RT filtering.

Use **undo rtfilter check-after-policy** to restore the default.

Syntax

rtfilter check-after-policy

undo rtfilter check-after-policy

Default

A device performs RT filtering on VPNv4 routes and then applies the export routing policy to the matching routes before advertisement.

Views

BGP IPv4 RT filter address family view

Predefined user roles

network-admin

Usage guidelines

By default, a device performs RT filtering on VPNv4 routes and then applies the export routing policy to the matching routes before advertisement. In some networks, no route targets are configured in the VPN instance, and the route targets of VPNv4 routes are configured through the export routing policy. If IPv4 RT filter route exchange is enabled for the device and its peer, all VPNv4 routes cannot pass RT filtering, and no VPNv4 routes can be advertised.

To resolve this issue, you can execute this command to configure the device to apply the export routing policy to VPNv4 routes before RT filtering.

Examples

Apply the export routing policy to VPNv4 routes before RT filtering.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] address-family ipv4 rtfilter
```

```
[Sysname-bgp-default-rtf-ipv4] rtfilter check-after-policy
```

New feature: Configuring a BJCA authentication server

Configuring a BJCA authentication server

About this task

Perform this task to define the following parameters for a BJCA authentication server:

- The URLs that the server uses to provide authentication services for users.
- The app ID of the application system used by the users.
- The preshared key used by the device to exchange AAA private protocol packets with the server.
- The VPN instance to which the server belongs.
- The response timeout time for the server.

You can specify a BJCA authentication server in an AAA private protocol scheme. The device can obtain the parameters required for communication with this BJCA authentication server for users that use the AAA private protocol scheme.

Restrictions and guidelines

You can specify a BJCA authentication server in multiple AAA private protocol schemes.

The system supports a maximum of 16 BJCA authentication servers.

On the initiator and responder of an IPsec tunnel, you must complete the following IKE settings:

- **Initiator**—Configure user information required for IKE authentication through an AAA server.
- **Responder**—Enable XAUTH client authentication and use the AAA private protocol for communication with IKE clients.

Procedure

1. Enter system view.

system-view

2. Create a BJCA authentication server and enter its view.

- aaa bjca-auth-server** *bjca-auth-server-name*
- Configure the URLs of the BJCA authentication server.
url { **get-random** | **get-token** | **token-auth** } *url-string*
 By default, the URLs of the BJCA authentication server are not configured.
 Configure the get-random URL and get-Token URL on the IPsec tunnel initiator, and configure the Token-authentication URL on the IPsec tunnel responder.
 - Configure the app ID of the BJCA authentication server.
appid *appid-string*
 By default, the app ID of the BJCA authentication server is not configured.
 Configure the app ID of the BJCA authentication server on the IPsec tunnel responder.
 - Specify the preshared key used for communication with the BJCA server.
key { **cipher** | **simple** } *string*
 By default, no preshared key is configured for the device to communicate with the BJCA server.
 Specify the preshared key used for communication with the BJCA server on the IPsec tunnel responder.
 - (Optional.) Specify the VPN instance to which the BJCA authentication server belongs.
vpn-instance *vpn-instance-name*
 By default, no VPN instance is specified for a BJCA authentication server.
 - (Optional.) Specify a PKI domain for communication with the BJCA authentication server.
pki-domain *domain-name*
 By default, no PKI domain is specified for communication with a BJCA authentication server.
 This step is required if the device acts as the IPsec tunnel initiator. You do not need to perform this step if the device acts as the IPsec tunnel responder.
 - (Optional.) Set the response timeout time for the BJCA authentication server.
timer response-timeout *seconds*
 By default, the response timeout time for a BJCA authentication server is 5 seconds.

Command reference

aaa bjca-auth-server

Use **aaa bjca-auth-server** to create a BJCA authentication server and enter its view, or enter the view of an existing BJCA authentication server.

Use **undo aaa bjca-auth-server** to delete a BJCA authentication server.

Syntax

aaa bjca-auth-server *bjca-auth-server-name*
undo aaa bjca-auth-server *bjca-auth-server-name*

Default

No BJCA authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

bjca-auth-server-name: Specifies a name for the BJCA authentication server, a case-insensitive string of 1 to 64 characters.

Usage guidelines

The device exchanges HTTP-based AAA private protocol packets with the BJCA authentication server to perform identity authentication for access endpoints.

You can specify the same BJCA authentication server in multiple AAA private protocol schemes.

The system supports a maximum of 16 BJCA authentication servers.

Examples

Create a BJCA authentication server named **bbb** and enter its view.

```
<Sysname> system-view
[Sysname] aaa bjca-auth-server bbb
[Sysname-bjca-auth-server-bbb]
```

Related commands

display aaa-private-protocol scheme

New feature: Enabling transparent transmission of LLDP frames

Enabling transparent transmission of LLDP frames

About this task

On an MPLS L2VPN network, you can enable transparent LLDP frame transmission on the PE interfaces connected to CEs so the CEs can establish neighbor relationships across the PEs.

An interface configured with this feature can transmit LLDP frames transparently, whether or not LLDP is enabled on it.

Restrictions and guidelines

Before you enable transparent LLDP frame transmission on a PE interface connected to a CE, disable LLDP on the interface to prevent the CE from establishing neighbor relationships with the PE and the resulting topology errors.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Enable transparent LLDP frame transmission on the interface.
lldp transparent enable
By default, transparent LLDP frame transmission is disabled on an interface.

Command reference

lldp transparent enable

Use **lldp transparent enable** to enable transparent transmission of LLDP frames on an interface.

Use **undo lldp transparent enable** to disable transparent transmission of LLDP frames on an interface.

Syntax

lldp transparent enable

undo lldp transparent enable

Default

Transparent transmission of LLDP frames is disabled on an interface.

Views

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

On an MPLS L2VPN network, you can enable transparent LLDP frame transmission on the PE interfaces connected to CEs so the CEs can establish neighbor relationships across the PEs.

Before you enable transparent LLDP frame transmission on a PE interface connected to a CE, disable LLDP on the interface to prevent the CE from establishing neighbor relationships with the PE and the resulting topology errors.

An interface configured with this feature can transmit LLDP frames transparently, whether or not LLDP is enabled on it.

Examples

```
# Enable transparent LLDP frame transmission on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lldp transparent enable
```

New feature: Transparent LACPDU transmission

Enabling transparent LACPDU transmission

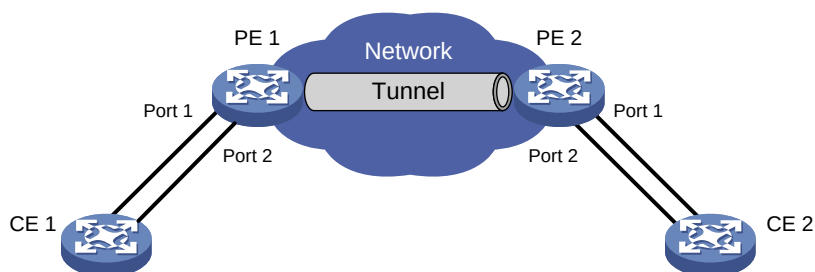
About this task

To establish a dynamic aggregation between two remote CEs in an L2VPN network, use transparent LACPDU transmission on the PEs to which the CEs are attached, as shown in [Figure 3](#).

This feature enables the PEs to forward LACPDUs for the CEs to establish a dynamic aggregation.

If this feature is disabled, the PEs terminate the LACPDUs. The remote CEs cannot establish dynamic aggregations.

Figure 3 Application scenario of transparent LACPDU transmission



Prerequisites

Perform the following tasks on PEs:

1. Configure the **untagged** or **default** frame match criterion for the Ethernet service instances on the interfaces connected to CEs.
2. Map the Ethernet service instances to different VSIs and set the access mode to Ethernet for the VSIs.

For more information about Ethernet service instances, see VPLS and MPLS L2VPN configuration in *MPLS Configuration Guide*.

Restrictions and guidelines

When you use this feature on the PEs, follow these guidelines:

- Enable transparent LACPDU transmission on the interfaces that transmit traffic between CEs and PEs and between PEs.
- Do not use an interface for dynamic link aggregation if you enable transparent LACPDU transmission on that interface. With transparent LACPDU transmission enabled, an interface cannot be selected for aggregation.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Enable transparent LACPDU transmission.
lacp transparent enable

By default, transparent LACPDU transmission is disabled.

Command reference

lacp transparent enable

Use **lacp transparent enable** to enable transparent LACPDU transmission on an interface.

Use **undo lacp transparent enable** to disable transparent LACPDU transmission on an interface.

Syntax

lacp transparent enable

undo lacp transparent enable

Default

Transparent LACPDU transmission is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

To establish a dynamic aggregation between two remote CEs in an L2VPN network, use transparent LACPDU transmission on the PEs to which the CEs are attached.

On the PEs, enable transparent LACPDU transmission on the interfaces that transmit traffic between CEs and PEs and between PEs.

Do not use an interface for dynamic link aggregation if you enable transparent LACPDU transmission on that interface. With transparent LACPDU transmission enabled, an interface cannot be selected for aggregation.

Examples

```
# Enable transparent LACPDU transmission on GigabitEthernet 1/0/1.
```

```
<Sysname> system
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lacp transparent enable
```

New feature: Configuring VLAN mapping

Configuring VLAN mapping

About VLAN mapping

VLAN mapping re-marks VLAN traffic with new VLAN IDs.

VLAN mapping types

H3C provides the following types of VLAN mapping:

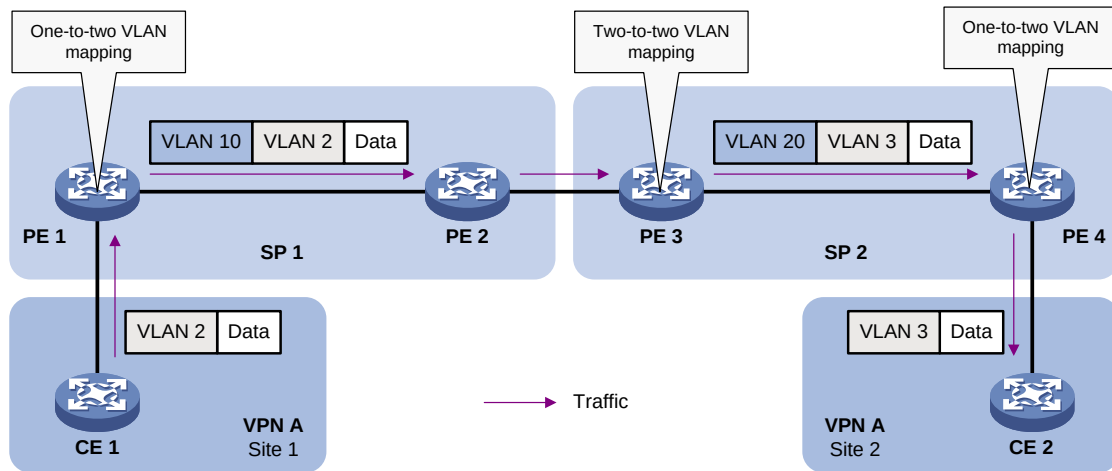
- **One-to-two VLAN mapping**—Tags single-tagged packets with an outer VLAN tag.
- **Zero-to-two VLAN mapping**—Adds double VLAN tags to untagged packets.
- **Two-to-two VLAN mapping**—Replaces the outer and inner VLAN IDs of double tagged traffic with a new pair of VLAN IDs.

VLAN mapping application scenarios

One-to-two and two-to-two VLAN mapping

One-to-two and two-to-two VLAN mapping are typically used to implement communication across different SP networks, as shown in [Figure 4](#)

Figure 4 Application scenario of one-to-two and two-to-two VLAN mapping



As shown in Figure 4, Site 1 and Site 2 of VPN A are in VLAN 2 and VLAN 3, respectively. The SP 1 network assigns SVLAN 10 to Site 1. The SP 2 network assigns SVLAN 20 to Site 2. When the packet from Site 1 arrives at PE 1, PE 1 tags the packet with SVLAN 10 by using one-to-two VLAN mapping.

When the double-tagged packet from the SP 1 network arrives at the SP 2 network interface, PE 3 processes the packet as follows:

- Replaces SVLAN tag 10 with SVLAN tag 20.
- Replaces CVLAN tag 2 with CVLAN tag 3.

One-to-two VLAN mapping provides the following benefits:

- Enables a customer network to plan its CVLAN assignment without conflicting with SVLANs.
- Adds a VLAN tag to a tagged packet and expands the number of available VLANs to 4094×4094 .
- Reduces the stress on the SVLAN resources, which were 4094 VLANs in the SP network before the mapping process was initiated.

Zero-to-two VLAN mapping

The application scenario of zero-to-two VLAN mapping is similar to the scenario of one-to-two VLAN mapping. Zero-to-two VLAN mapping is used on the customer-side port of a PE to add double tags to untagged packets.

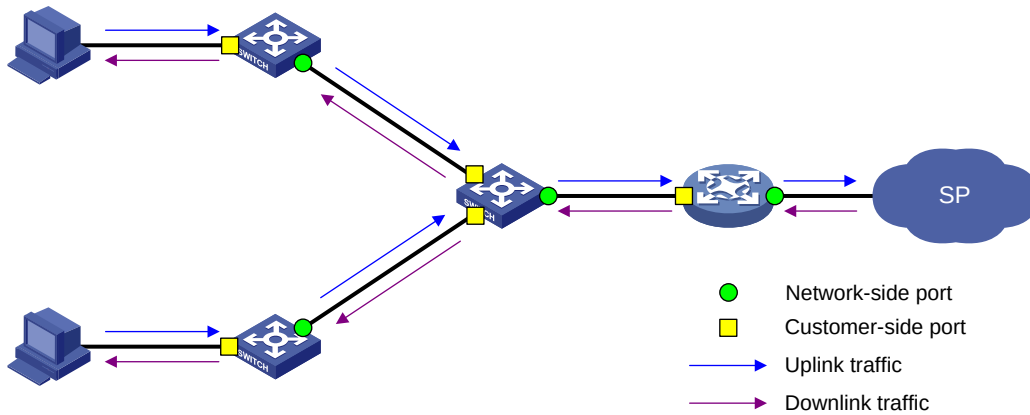
VLAN mapping implementations

Figure 5 shows a simplified network that illustrates basic VLAN mapping terms.

Basic VLAN mapping terms include the following:

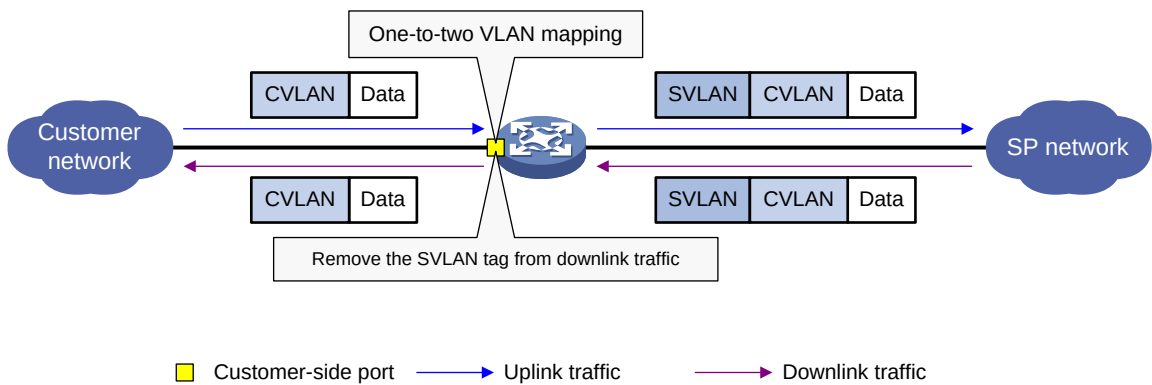
- **Uplink traffic**—Traffic transmitted from the customer network to the service provider network.
- **Downlink traffic**—Traffic transmitted from the service provider network to the customer network.
- **Network-side port**—A port connected to or closer to the service provider network.
- **Customer-side port**—A port connected to or closer to the customer network.

Figure 5 Basic VLAN mapping terms



One-to-two VLAN mapping

Figure 6 One-to-two VLAN mapping implementation



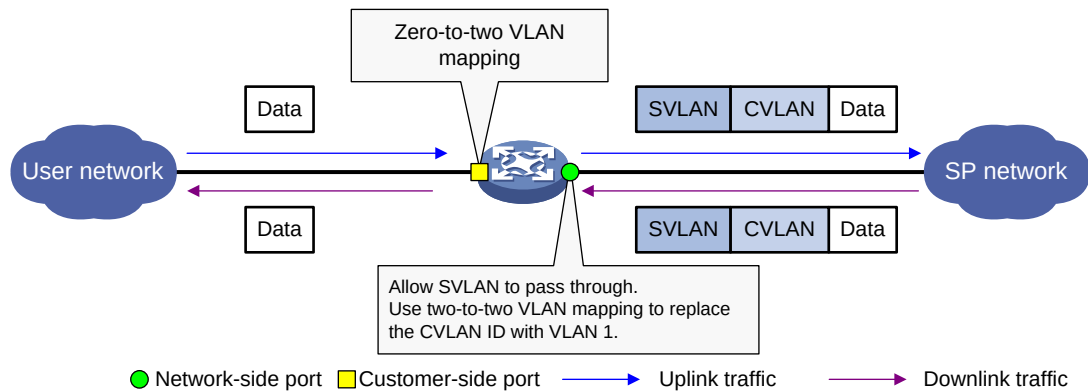
As shown in Figure 6, one-to-two VLAN mapping is implemented on the customer-side port to add the SVLAN tag for the uplink traffic.

For the downlink traffic to be correctly sent to the customer network, make sure the SVLAN tag is removed on the customer-side port before transmission. Use one of the following methods to remove the SVLAN tag from the downlink traffic:

- Configure the customer-side port as a hybrid port and assign the port to the SVLAN as an untagged member.
- Configure the customer-side port as a trunk port and set the port PVID to the SVLAN.

Zero-to-two VLAN mapping

Figure 7 Zero-to-two VLAN mapping implementation



As shown in Figure 7, zero-to-two VLAN mapping is implemented on the customer-side port to add double tags to untagged uplink traffic. For zero-to-two VLAN mapping to take effect, the port PVID must be VLAN 1.

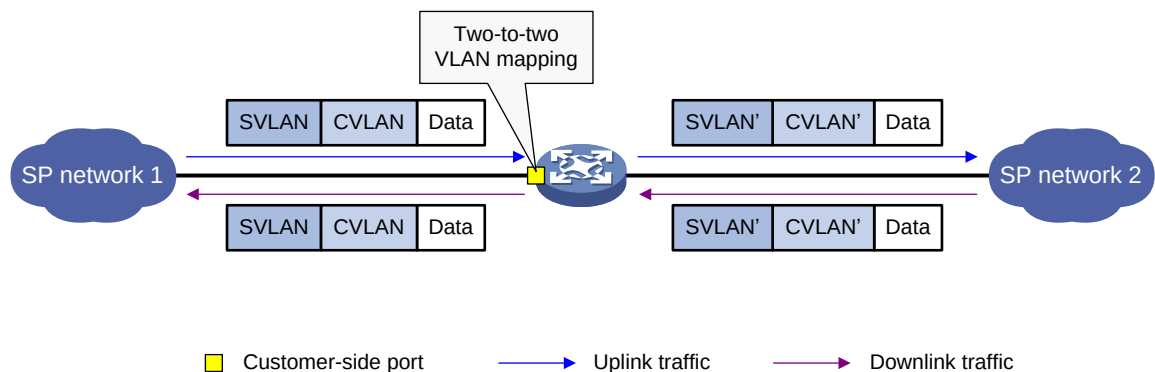
For correct downlink traffic transmission, the downlink traffic must be untagged or tagged with VLAN 1 when it is sent out of the customer-side port.

To tag the downlink traffic with VLAN 1:

2. Configure the network-side port to allow the traffic from the SVLAN to pass through.
3. If the CVLAN of the traffic is not VLAN 1, configure a two-to-two VLAN mapping on the network-side port to replace the CVLAN ID with VLAN 1.
4. Assign the customer-side port to the SVLAN as an untagged member.

Two-to-two VLAN mapping

Figure 8 Two-to-two VLAN mapping implementation



As shown in Figure 8, two-to-two VLAN mapping is implemented on the customer-side port and replaces VLAN tags as follows:

- Replaces the CVLAN and the SVLAN with the CVLAN' and the SVLAN' for the uplink traffic.
- Replaces the SVLAN' and CVLAN' with the SVLAN and the CVLAN for the downlink traffic.

Restrictions and guidelines: VLAN mapping configuration

To add VLAN tags to packets, you can configure both VLAN mapping and QinQ. VLAN mapping takes effect if a configuration conflict occurs. For more information about QinQ, see "Configuring QinQ."

To add or replace VLAN tags for packets, you can configure both VLAN mapping and a QoS policy. The QoS policy takes effect if a configuration conflict occurs. For information about QoS policies, see *ACL and QoS Configuration Guide*.

VLAN mapping tasks at a glance

Use the appropriate VLAN mapping methods for the devices in the network.

To configure VLAN mapping, perform the following tasks:

- **Configuring one-to-two VLAN mapping**
Configure one-to-two VLAN mapping on PE 1 and PE 4, as shown in [Figure 4](#), through which traffic from customer networks enters the service provider networks.
- **Configuring zero-to-two VLAN mapping**
Configure zero-to-two VLAN mapping on PE 1 and PE 4, as shown in [Figure 4](#), through which traffic from customer networks enters the service provider networks.
- **Configuring two-to-two VLAN mapping**
Configure two-to-two VLAN mapping on PE 3, as shown in [Figure 4](#), which is an edge device of the SP 2 network.

Prerequisites

Before you configure VLAN mapping, create original and translated VLANs.

Configuring one-to-two VLAN mapping

About this task

Configure one-to-two VLAN mapping on the customer-side ports of edge devices from which customer traffic enters SP networks, for example, on PEs 1 and 4 in [Figure 4](#).

One-to-two VLAN mapping enables the edge devices to add an SVLAN tag to each incoming packet.

Restrictions and guidelines

Only one SVLAN tag can be added to packets from the same CVLAN. To add different SVLAN tags to different CVLAN packets on a port, set the port link type to hybrid and configure multiple one-to-two VLAN mappings.

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet in the service provider network.

Procedure

1. Enter system view.
system-view
2. Enter VEB interface view.

interface ve-bridge *interface-number*

3. Set the link type of the port.

port link-type { **hybrid** | **trunk** }

By default, the link type of a port is **access**.

4. Assign the port to the CVLANs.

- Assign the trunk port to the CVLANs.

port trunk permit vlan *vlan-id-list*

By default, a trunk port is assigned to VLAN 1.

- Assign the hybrid port to the CVLANs.

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.

5. Configure the port to allow packets from the SVLAN to pass through untagged.

- Configure the SVLAN as the PVID of the trunk port and assign the trunk port to the SVLAN.

port trunk pvid vlan *vlan-id*

port trunk permit vlan { *vlan-id-list* | **all** }

- Assign the hybrid port to the SVLAN as an untagged member.

port hybrid vlan *vlan-id-list* **untagged**

6. Configure a one-to-two VLAN mapping.

vlan mapping nest { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id*

By default, no VLAN mapping is configured on an interface.

Configuring zero-to-two VLAN mapping

About this task

Configure zero-to-two VLAN mapping on PE 1 and PE 4, as shown in [Figure 4](#), through which traffic from customer networks enters the service provider networks.

Restrictions and guidelines

- For zero-to-two VLAN mapping to take effect, set the PVID of the customer-side port to 1.
- If the CVLAN ID of the downlink traffic is not VLAN 1, configure a two-to-two VLAN mapping on the network-side port to change the CVLAN ID to 1.
- As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the double-tagged packet in the service provider network.

Procedure

1. Enter system view.

system-view

2. Enter VEB interface view.

interface ve-bridge *interface-number*

3. Set the port link type to hybrid.

port link-type **hybrid**

By default, the link type of a port is **access**.

4. Set the port PVID to VLAN 1.

port hybrid pvid **vlan 1**

By default, the PVID of a hybrid port is the ID of the VLAN to which the port belongs when its link type is **access**.

5. Assign the port to VLAN 1.

port hybrid vlan *vlan-id-list* { tagged | untagged }

By default, a hybrid port is an untagged member of VLAN 1.

6. Assign the port to the SVLAN as an untagged member.

port hybrid vlan *vlan-id-list* untagged

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.

7. Configure a zero-to-two VLAN mapping.

vlan mapping untagged nested-outer-vlan *outer-vlan-id* nested-inner-vlan *inner-vlan-id*

By default, no VLAN mapping is configured on an interface.

Configuring two-to-two VLAN mapping

About this task

Configure two-to-two VLAN mapping on the customer-side port of an edge device that connects two SP networks, for example, on PE 3 in [Figure 4](#). Two-to-two VLAN mapping enables two sites in different VLANs to communicate at Layer 2 across two service provider networks that use different VLAN assignment schemes.

Procedure

1. Enter system view.

system-view

2. Enter VEB interface view.

interface ve-bridge *interface-number*

3. Set the link type of the port.

port link-type { hybrid | trunk }

By default, the link type of a port is **access**.

4. Assign the port to the original VLANs and the translated VLANs.

- Assign the trunk port to the original VLANs and the translated VLANs.

port trunk permit vlan *vlan-id-list*

By default, a trunk port is assigned to VLAN 1.

- Assign the hybrid port to the original VLANs and the translated VLANs as a tagged member.

port hybrid vlan *vlan-id-list* tagged

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.

5. Configure a two-to-two VLAN mapping.

vlan mapping tunnel *outer-vlan-id* *inner-vlan-id* translated-vlan *outer-vlan-id* *inner-vlan-id*

By default, no VLAN mapping is configured on an interface.

VLAN mapping commands

display vlan mapping

Use **display vlan mapping** to display VLAN mapping information.

Syntax

display vlan mapping [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, the command displays VLAN mapping information on all interfaces.

Examples

Display VLAN mapping information on all interfaces.

```
<Sysname> display vlan mapping
Interface VE-Bridge1/1/0/0:
  Outer VLAN      Inner VLAN      Translated Outer VLAN      Translated Inner VLAN
  1                3                8                            9
  3-5              N/A                9                            3-5
```

Table 40 Command output

Field	Description
Interface	Information of the interface.
Outer VLAN	Original outer VLAN. - This field indicates the original VLAN for one-to-two VLAN mapping. - This field displays N/A for zero-to-two VLAN mapping
Inner VLAN	Original inner VLAN. - This field displays N/A for one-to-two VLAN mapping. - This field displays N/A for zero-to-two VLAN mapping.
Translated Outer VLAN	Translated outer VLAN. This field indicates the SVLAN to be added for zero-to-two VLAN mapping.
Translated Inner VLAN	Translated inner VLAN. This field indicates the CVLAN to be added for zero-to-two VLAN mapping.

Related commands

vlan mapping

vlan mapping

Use **vlan mapping** to configure VLAN mapping on an interface.

Use **undo vlan mapping** to cancel the VLAN mapping configuration.

Syntax

vlan mapping { **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **tunnel** *outer-vlan-id* *inner-vlan-id* **translated-vlan** *outer-vlan-id* *inner-vlan-id* }

undo vlan mapping { **all** | **nest** { **range** *vlan-range-list* | **single** *vlan-id-list* } **nested-vlan** *vlan-id* | **tunnel** *outer-vlan-id* *inner-vlan-id* **translated-vlan** *outer-vlan-id* *inner-vlan-id* }

Default

No VLAN mapping is configured on an interface.

Views

VEB interface view

Predefined user roles

network-admin

Parameters

nest range *vlan-range-list* **nested-vlan** *vlan-id*: Specifies the CVLAN ranges and the SVLAN for a one-to-two VLAN mapping. The *vlan-range-list* argument specifies a space-separated list of up to 10 CVLAN items. Each item specifies a CVLAN ID or a range of CVLAN IDs in the format of *vlan-id1* to *vlan-id2*. The value range for CVLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument. Different CVLAN ranges cannot overlap. The *vlan-id* argument specifies the SVLAN ID in the range of 1 to 4094.

nest single *vlan-id-list* **nested-vlan** *vlan-id*: Specifies the CVLANs and the SVLAN for a one-to-two VLAN mapping. The *vlan-id-list* argument specifies a space-separated list of up to 10 CVLAN IDs, each of which is in the range of 1 to 4094. The *vlan-id* argument specifies the SVLAN ID in the range of 1 to 4094.

tunnel *outer-vlan-id* *inner-vlan-id* **translated-vlan** *outer-vlan-id* *inner-vlan-id*: Specifies the original outer VLAN ID, original inner VLAN ID, translated outer VLAN ID, and translated inner VLAN ID for a two-to-two VLAN mapping. The value ranges for the *outer-vlan-id* argument and the *inner-vlan-id* argument are both 1 to 4094.

all: Deletes all VLAN mapping configurations from the interface.

Usage guidelines

VLAN mapping takes effect only on VLAN-tagged packets received on an interface.

The original and translated VLANs in VLAN mappings on an interface must meet the following requirements:

- Different types of VLAN mapping entries cannot include the same original VLANs or translated VLANs.
- Different two-to-two VLAN mapping entries cannot include the same translated VLANs. If you configure multiple two-to-two VLAN mapping entries for the same original VLANs, only the first configuration takes effect.

The configuration restrictions between QinQ and VLAN mappings are as follows:

- Before you enable or disable QinQ on a port, you must remove all VLAN mappings on the port.
- You cannot configure two-to-two VLAN mappings on a QinQ-enabled port.

If you use both transparent VLANs and VLAN mappings on an interface, the transparent VLANs cannot be the following VLANs:

- Original or translated VLANs of one-to-two VLAN mappings.
- Original or translated outer VLANs of two-to-two VLAN mappings.

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet on the service provider network.

Examples

Configure one-to-two VLAN mappings on VE-Bridge 1/0/1 to add SVLAN tag 101 to packets carrying VLAN tags 1 through 10 and VLAN tag 80.

```
<Sysname> system-view
[Sysname] interface ve-bridge 1/0/1
[Sysname-VE-Bridge1/0/1] vlan mapping nest range 1 to 10 nested-vlan 101
[Sysname-VE-Bridge1/0/1] vlan mapping nest single 80 nested-vlan 101
```

Configure a two-to-two VLAN mapping on VE-Bridge 1/0/1 to map SVLAN 101 and CVLAN 1 to SVLAN 201 and CVLAN 10.

```
<Sysname> system-view
[Sysname] interface ve-bridge 1/0/1
[Sysname-VE-Bridge1/0/1] vlan mapping tunnel 101 1 translated-vlan 201 10
```

Related commands

display vlan mapping

vlan mapping untagged

Use **vlan mapping untagged** to configure zero-to-two VLAN mapping on an interface.

Use **undo vlan mapping untagged** to remove the zero-to-two VLAN mapping configuration.

Syntax

vlan mapping untagged nested-outer-vlan *outer-vlan-id* **nested-inner-vlan** *inner-vlan-id*

undo vlan mapping untagged

Default

No zero-to-two VLAN mapping is configured on an interface.

Views

VEB interface view

Predefined user roles

network-admin

Parameters

nested-outer-vlan *outer-vlan-id*: Specifies the SVLAN ID in the range of 1 to 4094.

nested-inner-vlan *inner-vlan-id*: Specifies the CVLAN ID in the range of 1 to 4094.

Usage guidelines

This command takes effect only on ports that use VLAN 1 as the PVID.

Before you modify a zero-to-two VLAN mapping, first execute the **undo vlan mapping untagged** command to remove the previous configuration.

As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the double-tagged packet in the service provider network.

Examples

Configure a zero-to-two VLAN mapping on VE-Bridge 1/0/1 to add SVLAN 200 and CVLAN 100 to untagged packets.

```
<Sysname> system-view
[Sysname] interface ve-bridge 1/0/1
[Sysname-VE-Bridge1/0/1] vlan mapping untagged nested-outer-vlan 200 nested-inner-vlan
100
```

Related commands

display vlan mapping

New feature: PKI domain for communication with a JIT authentication server

Specifying a PKI domain for communication with a JIT authentication server

pki-domain

Use **pki-domain** to specify a PKI domain for communication with a JIT authentication server.

Use **undo pki-domain** to restore the default.

Syntax

pki-domain *domain-name*

undo pki-domain

Default

No PKI domain is specified for communication with a JIT authentication server.

Views

JIT authentication server view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

When the device acts as the IPsec tunnel initiator to send a token request to the JIT or BJCA authentication server, it obtains a local digital certificate based on the specified PKI domain. The local digital certificate is used to add a digital signature to some critical data in the request packet. Then, the device sends the packet that includes the digital signature to the server. When the server receives the token request packet, it validates the signature information in the packet.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify PKI domain **jit-domain** for communication with the JIT authentication server named **ccc**.

```
<Sysname> system-view
[Sysname] aaa jit-auth-server ccc
```

New feature: SDWAN

About SDWAN

Software-defined WAN (SDWAN) is a VPN technology that applies SDN technologies to WAN. The control plane uses SSL and MP-BGP to advertise transport tunnel endpoint (TTE) information to set up SDWAN tunnels between sites and uses MP-BGP to advertise private routes between sites. The data plane uses UDP to encapsulate and forward data packets and uses security mechanisms such as IPsec to secure data transmission. SDWAN provides secure and reliable interconnection services for geographically dispersed enterprise networks and data centers.

Restrictions: Licensing requirements for SDWAN

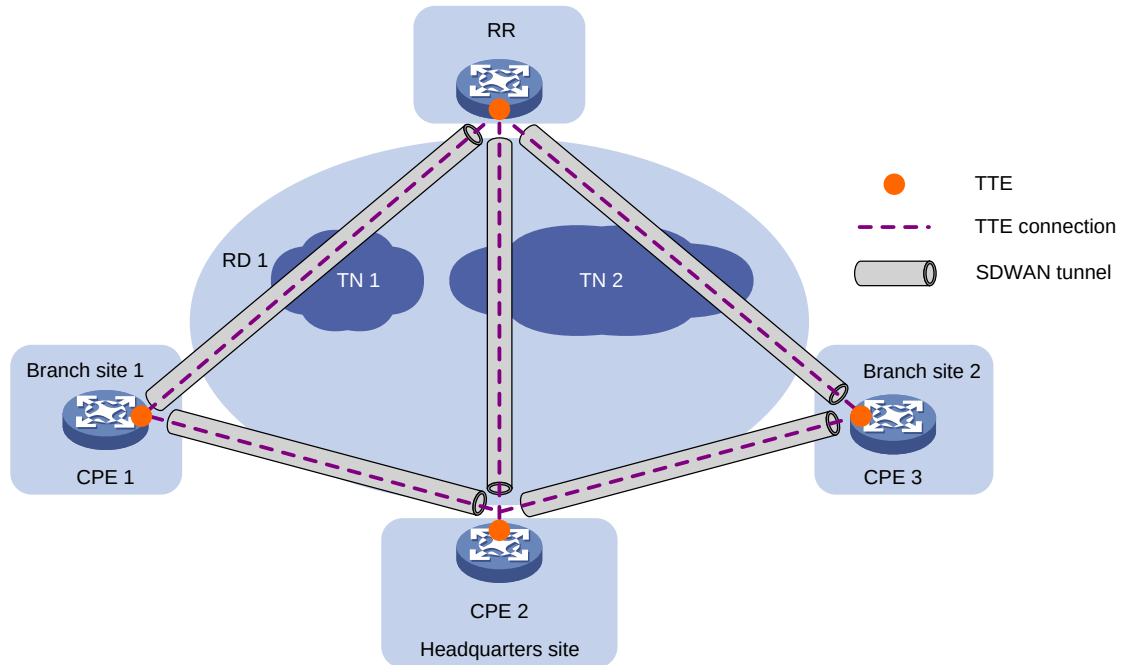
SDWAN requires a license to run on the device. For information about feature licensing, see license management in *Fundamentals Configuration Guide*.

SDWAN network model

As shown in [Figure 9](#), SDWAN contains the following components:

- **Customer provided edge (CPE)**—Edge device at a customer site.
- **Route reflector (RR)**—Used to reflect TTE information and private routes between CPEs.
- **Transport network (TN)**—Service provider WAN that connects sites. A transport network can be a service provider VPN or the Internet public network. A transport network is identified by its transport network ID or name. Transport networks are the fundamentals to construct SDWAN overlay network.
- **Routing domain (RD)**—Domain that contains transport networks that are reachable at Layer 3. SDWAN tunnels can be established only between CPEs or between CPEs and RRs in the same routing domain.
- **Site ID**—A site ID is a string of digits used to uniquely identify a site in the SDWAN network. The network controller allocates site IDs to all sites.
- **Device ID**—A device ID uniquely identifies an SDWAN-capable device (or SDWAN device) at a site. Typically, a site contains one or two SDWAN devices.
- **SDWAN tunnel**—Point-to-multipoint logical channel established among SDWAN devices. One site transmits traffic to another site over an SDWAN tunnel.
- **Secure Sockets Layer (SSL) connection**—In the SDWAN network, a CPE and an RR establish an SSL connection to exchange TTE information for control channel establishment.
- **Transport tunnel endpoint (TTE)**—Endpoint that connects an SDWAN device to a transport network and endpoint of an SDWAN tunnel. Device TTE information includes the site ID, transport network ID (TN ID), private IP address, public IP address, and tunnel encapsulation mode.
- **TTE connection**—Point-to-point logical connection established between TTEs. An SDWAN tunnel can hold multiple TTE connections.

Figure 9 SDWAN network model



SDWAN packet formats

SDWAN supports control packets and data packets.

- SDWAN control packets are used for NAT traversal. The device uses SDWAN control packets to advertise its public IP address translated after NAT to remote devices. For more information about NAT traversal, see "[For more information about SDWAN tunnel establishment with NAT traversal.](#)"
- SDWAN data packets are used to forward user packets.

Control packet format

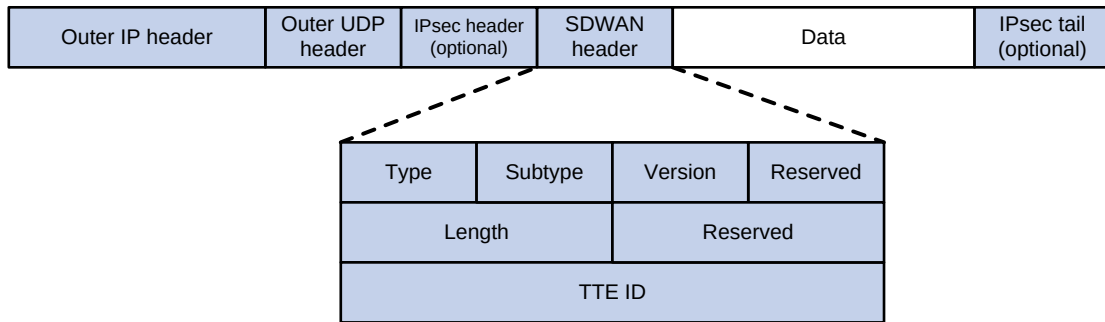
As shown in Figure 10, an SDWAN control packet contains the following components:

- Data portion.
- IPsec header (optional).
- 12-byte SDWAN header.
- 8-byte outer UDP header. The destination port number in the UDP header is the SDWAN UDP port number. By default, the port number is 4799.
- 20-byte outer IP header.

The SDWAN header contains the following fields:

- **Type**—Type of the packet. The length for this field is 8 bits. For an SDWAN control packet, the value is 1.
- **Subtype**—Subtype of the control packet. The length for this field is 8 bits. If the value is 1, the packet is a NAT address probe request packet.
- **Version**—Version number of SDWAN protocol packets. The value is fixed at 0.
- **Reserved**—Reserved field. The value is fixed at 0.
- **Length**—Length of the SDWAN header. The length for this field is 16 bits. The value is fixed at 12 in the current software version.
- **TTE ID**—Identifies a TTE. The length for this field is 32 bits.

Figure 10 SDWAN control packet format



Data packet format

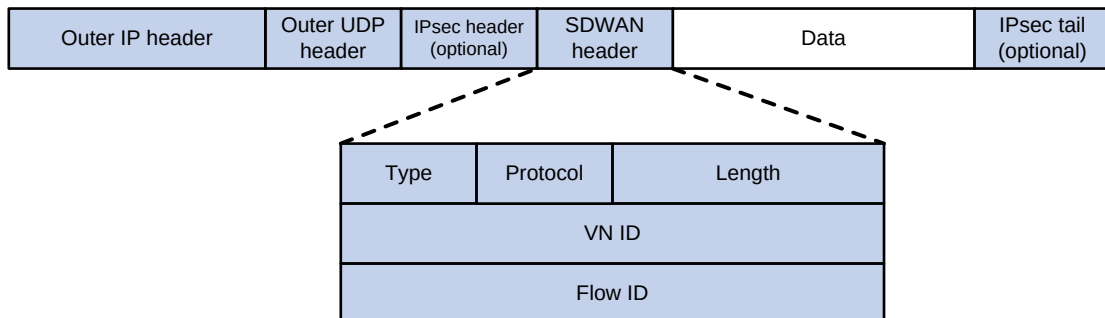
As shown in Figure 11, an SDWAN data packet contains the following components:

- Original data packet.
- IPsec header (optional).
- 12-byte SDWAN header.
- 8-byte outer UDP header. The destination port number in the UDP header is the SDWAN UDP port number. By default, the port number is 4799.
- 20-byte outer IP header.

The SDWAN header contains the following fields:

- **Type**—Type of the packet. The length for this field is 8 bits. For an SDWAN data packet, the value is 2.
- **Protocol**—Type of the inner data packet. The length for this field is 8 bits. If the value is 1, the packet is an IPv4 packet. If the value is 2, the packet is an IPv6 packet.
- **Length**—Length of the SDWAN header. The length for this field is 16 bits. The value is fixed at 12 in the current software version.
- **VN ID**—VN ID of the VPN instance to which the SDWAN data packet belongs. The length for this field is 32 bits. If the packet belongs to the public instance, the value for this field is all zeros.
- **Flow ID**—Flow ID of the SDWAN data packet. The length for this field is 32 bits. To mark packets with a flow ID, use the **remark flow-id** command. If no flow ID is marked, the value for this field is all zeros. For more information about the **remark flow-id** command, see QoS commands in *ACL and QoS Command Reference*.

Figure 11 SDWAN data packet format



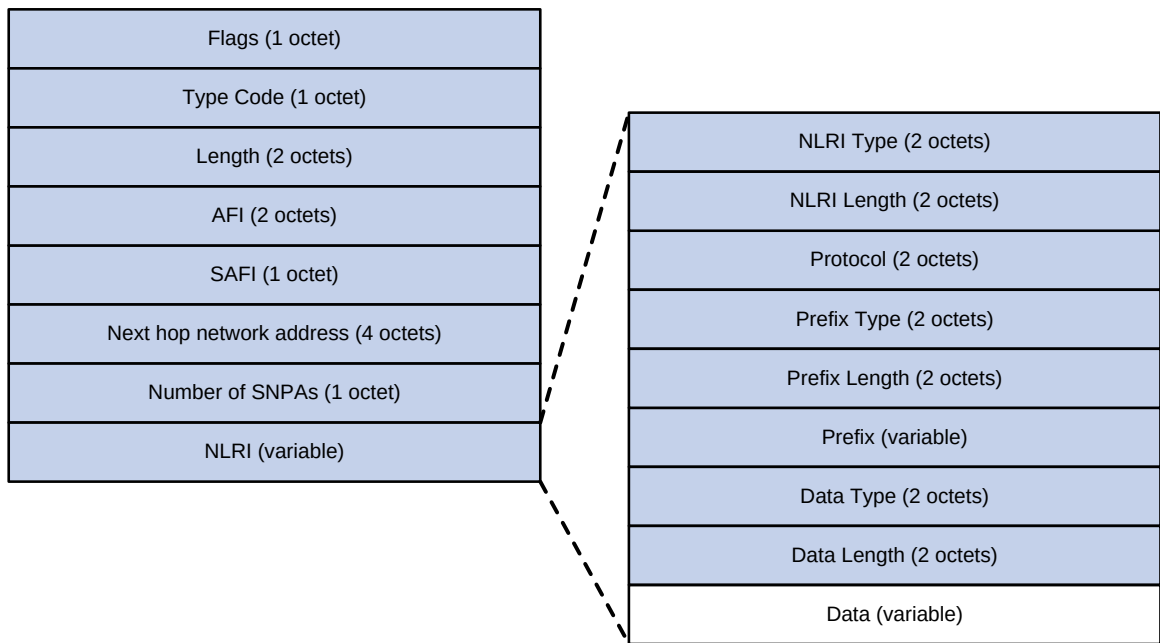
BGP extensions

BGP IPv4 tunnel-encap-ext address family

To support SDWAN, BGP defines a new address family called BGP IPv4 tunnel-encap-ext address family. This address family is a subsequent address family of the IPv4 address family. The subsequent address family identifier (SAFI) is 74. Routes exchanged under this address family are IPv4 tunnel-encap-ext routes. IPv4 tunnel-encap-ext routes can include the following information in the Multiprotocol Reachable NLRI (MP_REACH_NLRI) attribute:

- **TTE information**—Includes site ID, transport network ID, public IP address, private IP address, tunnel encapsulation mode, and QoS information. CPEs use the information to set up data channels between each other.
- **SaaS path quality information**—Includes link delay, jitter, packet loss ratio, and CQI. RIR uses the information to select the optimal path for application traffic.

Figure 12 MP_REACH_NLRI attribute in IPv4 tunnel-encap-ext routes



As shown in Figure 12, the MP_REACH_NLRI attribute in IPv4 tunnel-encap-ext routes contains the following fields:

- **Flags**—BGP attribute flags. The value is 0x90, which indicates that this attribute is an optional nontransitive attribute that includes complete information.
- **Type Code**—BGP attribute type. The value is 14.
- **Length**—Length of the MP_REACH_NLRI attribute.
- **AFI**—Address family identifier. The value is 1, which represents IPv4 address family.
- **SAFI**—Subsequent address family identifier. The value is 74, which represents IPv4 tunnel-encap-ext address family.
- **Next hop network address**—Next hop IP address.
- **Number of SNPAs**—Number of Subnetwork Point of Attachments (SNPAs) in the subsequent field. If the value is 0, the attribute does not include an SNPA.
- **NLRI**—Network layer reachability information.

Network layer reachability information in the MP_REACH_NLRI attribute includes the following fields:

- **NLRI Type**—Type of NLRI. If the value is 1, this field includes IPv4 TTE information. If the value is 2, this field includes SaaS path quality information. If the value is 3, this field includes IPv6 TTE information. If the value is 4, this field includes QoS TTE information.
- **NLRI Length**—Length of NLRI.
- **Protocol**—Protocol stack of NLRI. The value is 2.
- **Prefix Type**—Prefix type of NLRI. The value is 1.
- **Prefix Length**—Prefix length of NLRI.
- **Prefix**—Prefix information of NLRI. For TTE information, the value is the TTE ID. For SaaS path quality information, the value is the site ID and device ID.
- **Data Type**—Type of the data portion in NLRI. The value is 2.
- **Data Length**—Length of the data portion in NLRI.
- **Data**—Data portion in NLRI. This field includes detailed TTE information or SaaS path quality information.

BGP EVPN routes

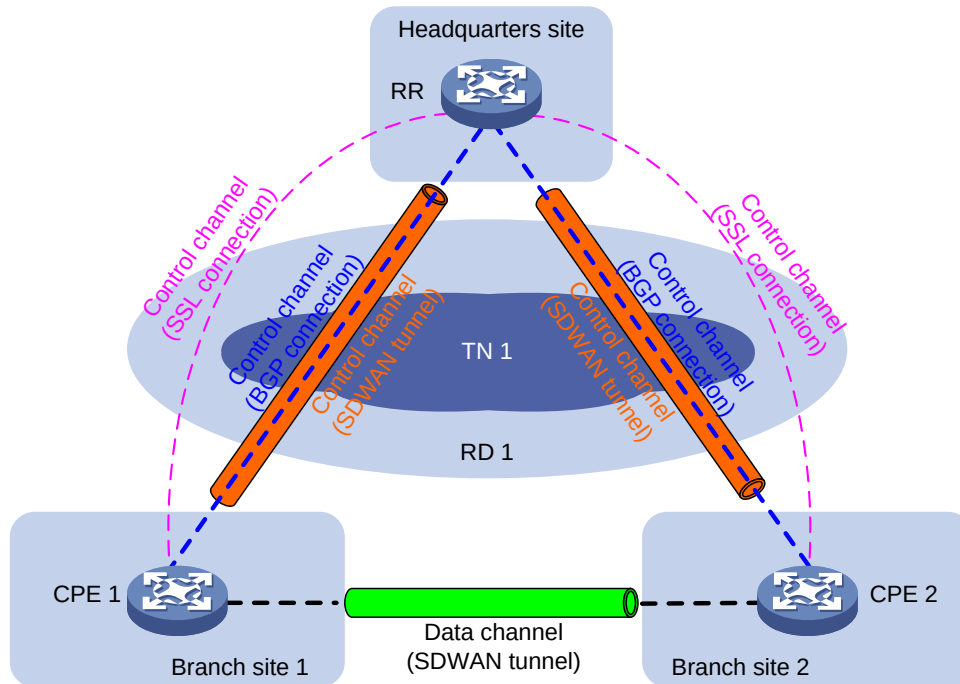
You can deploy SDWAN across VPNs. A CPE advertises VPN routes to other CPEs in the format of BGP EVPN IP prefix advertisement routes. To support SDWAN, the following extensions are added to BGP EVPN routes:

- SDWAN encapsulation is added to the TUNNEL_ENCAPSULATION_ATTRIBUTE attribute. SDWAN-encapsulated IP prefix advertisement routes can be forwarded only between the devices that are enabled to advertise BGP EVPN routes in SDWAN encapsulation.
- A VN ID is added to the NLRI field of IP prefix advertisement routes. The VN ID is used to differentiate private routes in different VPN instances.

Channel establishment

As shown in Figure 13, an SDWAN network supports control channels and data channels.

Figure 13 SDWAN channels



Control channel establishment

A control channel is established between an RR and a CPE to advertise TTE information and private routes. The establishment process is as follows:

1. The CPE and RR establish an SSL connection (control channel). The CPE is the SSL client, also referred to as the SDWAN client. The RR is the SSL server, also referred to as the SDWAN server.
2. The CPE and RR exchange TTE information.
3. After receiving TTE information from each other, the CPE and RR compare the routing domain, group ID, and transport network in the received TTE information with those in the local TTE information.
 - If the routing domains, group IDs, and transport networks are the same, the CPE and RR establish an SDWAN tunnel (control channel) between them.
 - If the routing domains, group IDs, or transport networks are different, the CPE and RR do not establish an SDWAN tunnel between them.
4. The CPE and RR each automatically add the user network routes (UNRs) destined for the system IP address of the peer device to the local routing table.
5. The CPE and RR establish a BGP connection (control channel) under the IPv4 tunnel-encap-ext address family based on their system IP addresses.

Data channel establishment

A data channel is established between two CPEs to transmit data packets. The establishment process is as follows:

1. The CPEs use IPv4 tunnel-encap-ext routes to advertise TTE information to an RR.
2. The RR reflects the TTE information of each CPE to the other CPE.
3. When each CPE receives TTE information reflected by the RR, they store the TTE information.

4. Each CPE sends the VPN routes learned from the local site to the RR through SDWAN-encapsulated IP prefix advertisement routes.
5. The RR reflects the IP prefix advertisement routes received from a CPE to the other CPE.
6. Each CPE looks up the locally stored TTE information for an IP prefix advertisement route reflected by the RR based on the next hop address of that route. If a matching TTE information entry is found, the CPE compares the routing domain, group ID, and transport network in the matching TTE information with the local routing domain, group ID, and transport network.
 - o If the routing domains, group IDs, and transport networks are all the same, the CPE establishes a connection to the TTE and establishes an SDWAN tunnel for the TTE connection.
 - o If the routing domains, group IDs, or transport networks are different, the CPE does not establish a connection to the TTE or establish an SDWAN tunnel.

To secure data transmission, use IPsec to encrypt data packets.

If the RR fully reflects IP prefix advertisement routes, each pair of CPEs in the same routing domain will establish SDWAN tunnels. In such a network, all sites can access one another. Potential data security risks exist. In addition, excessive number of devices in a routing domain brings great pressure on device performance and network bandwidth.

To resolve the above mentioned issues, the network administrator can configure export routing policies to filter IPv4 tunnel-encap-ext routes or SDWAN-encapsulated IP prefix advertisement routes on the RR. With the policies, the RR selectively reflects TTE information and IP prefix advertisement routes only to some of the CPEs. Only CPEs received the TTE information and IP prefix advertisement routes can establish SDWAN tunnels between them. CPEs that do not receive the TTE information or IP prefix advertisement routes cannot establish SDWAN tunnels. In this way, the SDWAN devices can establish SDWAN tunnels on demand. Establishing SDWAN tunnels on demand not only conserves device resources, but also isolates tenants by not establishing tunnels for them.

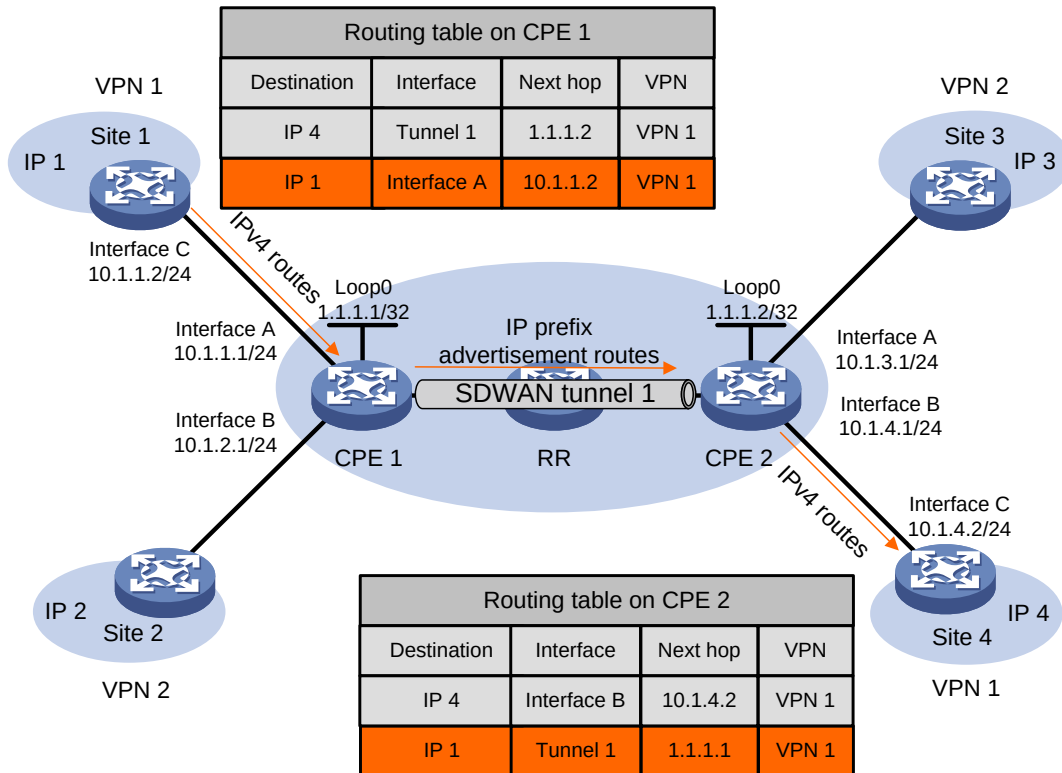
Route advertisement

As shown in Figure 14, inter-site route advertisement in an SDWAN network includes the following processes:

1. Each site advertises private routes to its local CPE.
2. CPEs advertise routes to each other.
3. Each CPE advertises private routes received from another site to its local site.

Then, the sites have routes to reach one another.

Figure 14 Route advertisement



Advertising private routes from local site to local CPE

The local site uses static routing, RIP, RIPng, OSPF, OSPFv3, IS-IS, IPv6 IS-IS, EBGp, or IBGP to advertise the private routes of the local site to the local CPE. The routes are standard IPv4 or IPv6 routes.

Advertising routes from local CPE to remote CPEs

1. When the local CPE learns private routes from the local site, it stores the routes to the routing table of the corresponding VPN instance.
2. The CPE adds RD and export targets to the standard IPv4 or IPv6 routes, converts the routes to BGP EVPN IP prefix advertisement routes, and advertises the routes to an RR. The next hop address of the routes is the system IP address of the local CPE.
3. The RR reflects the received IP prefix advertisement routes to remote CPEs.
4. When a remote CPE receives the IP prefix advertisement routes reflected by the RR, it matches the export targets in the IP prefix advertisement routes with the import targets of local VPN instances. If a matching VPN instance is found, the remote CPE accepts the IP prefix advertisement routes and adds the routes to the routing table of the VPN instance.

Advertising routes from remote CPEs to remote sites

The supported routing methods are the same as the routing methods for advertising routes from the local site to the local CPE. A remote site can use multiple methods to learn private routes from its CPE. The methods include static routing, RIP, RIPng, OSPF, OSPFv3, IS-IS, IPv6 IS-IS, EBGp, and IBGP.

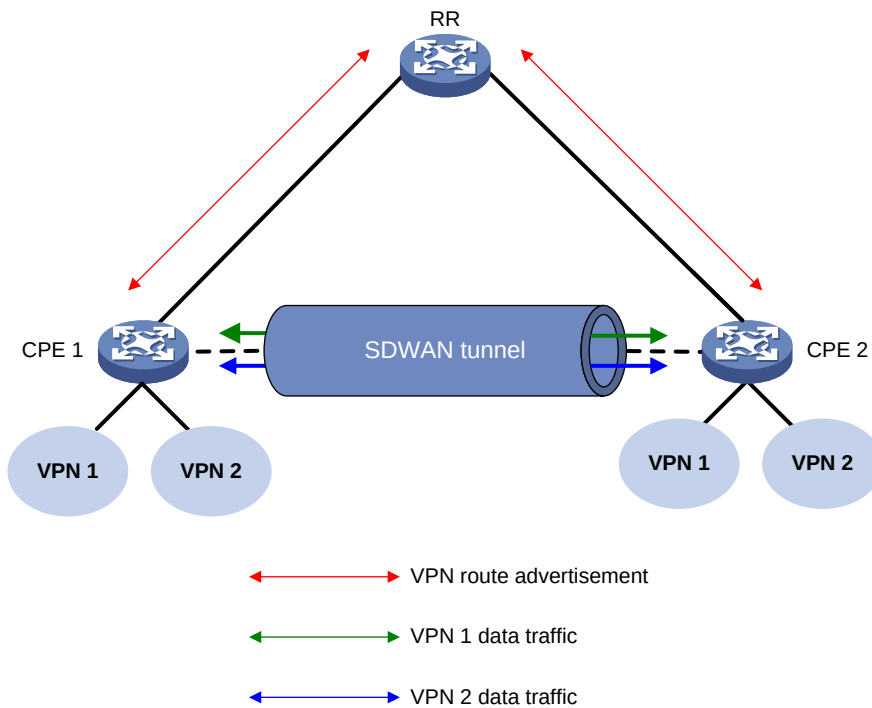
Traffic forwarding

In an SDWAN network, when a CPE receives a customer packet, it looks up the routing table for the output interface and next hop based on the destination IP address of the packet. The CPE forwards the packet differently according to the output interface.

- If the output interface is a local interface on the CPE, the CPE directly forwards the packet out of the interface to the next hop according to the forwarding table.
- If the output interface is an SDWAN tunnel interface, the CPE forwards the packet as follows:
 - a. Obtains the TTE ID of the next hop address according to the next hop address in the forwarding table.
 - b. Obtains TTE connection information based on the TTE IDs of the local device and next hop.
 - c. Adds SDWAN encapsulation to the packet according to the TTE connection information. The SDWAN header includes the VN ID of the VPN instance to which the data packet belongs. Packets of different VPN instances can be recurred to the same SDWAN tunnel. In this case, the VN ID in the SDWAN header is used to differentiate the VPN instances, as shown in Figure 15.
 - d. Forwards the packet out of the physical output interface bound to the SDWAN tunnel.

When the remote CPE receives and decapsulates the SDWAN packet, it looks up the routing table of the matching VPN instance according to the VN ID and forwards the packet.

Figure 15 SDWAN traffic forwarding



IPsec-protected SDWAN tunnels

To ensure confidentiality and integrity for data transmitted over SDWAN tunnels, the device supports using IPsec to protect SDWAN packets. For this purpose, the following extensions are added to IPsec:

- SDWAN IPsec profile.
- Sharing a pair of IPsec SAs among multiple SDWAN tunnels.

SDWAN tunnel establishment with NAT traversal

About this feature

As shown in Figure 16, users at branch sites use private IP addresses so as to conserve IP address resources. After NAT devices translate the private IP addresses to public IP addresses, users at one branch site can access other sites.

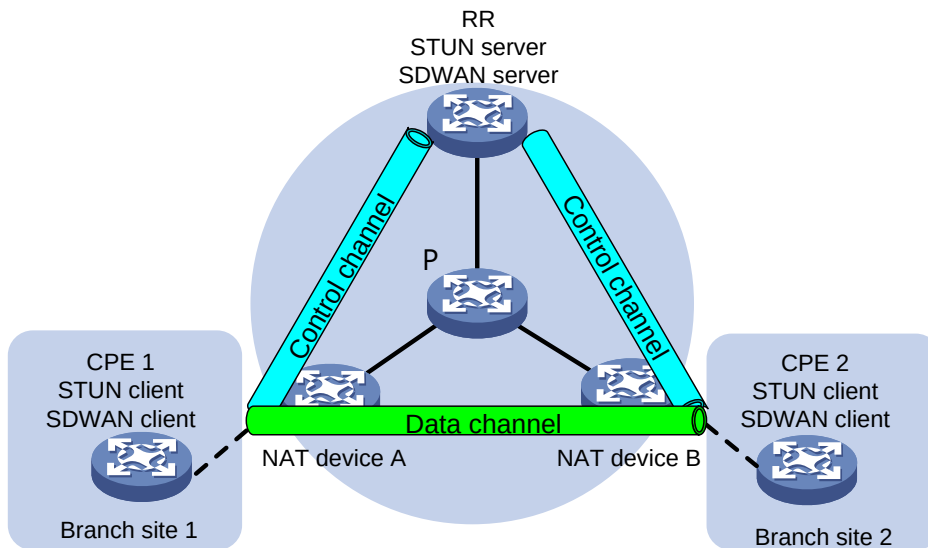
IP addresses of the packets sent by a CPE will change after the packets pass through a NAT device. If the CPE cannot obtain its post-NAT public IP address, it cannot establish an SDWAN tunnel with the other CPE or with the RR. To resolve this issue, use one of the following methods:

- Configure Session Traversal Utilities for NAT (STUN) in the SDWAN network. For more information about STUN, see *Layer 3—IP Services Configuration Guide*.
- Specify the post-NAT public IP address and port number for the source IP address and port number of tunneled packets on the CPE. If the RR is behind a NAT device, perform this task on the RR.

STUN uses the client/server model. Typically, use CPEs as STUN clients and use the RR as the STUN server. The clients exchange packets with the server to identify whether NAT devices exist in the SDWAN network. If NAT devices exist, the clients obtain their public IP addresses and port numbers translated after NAT.

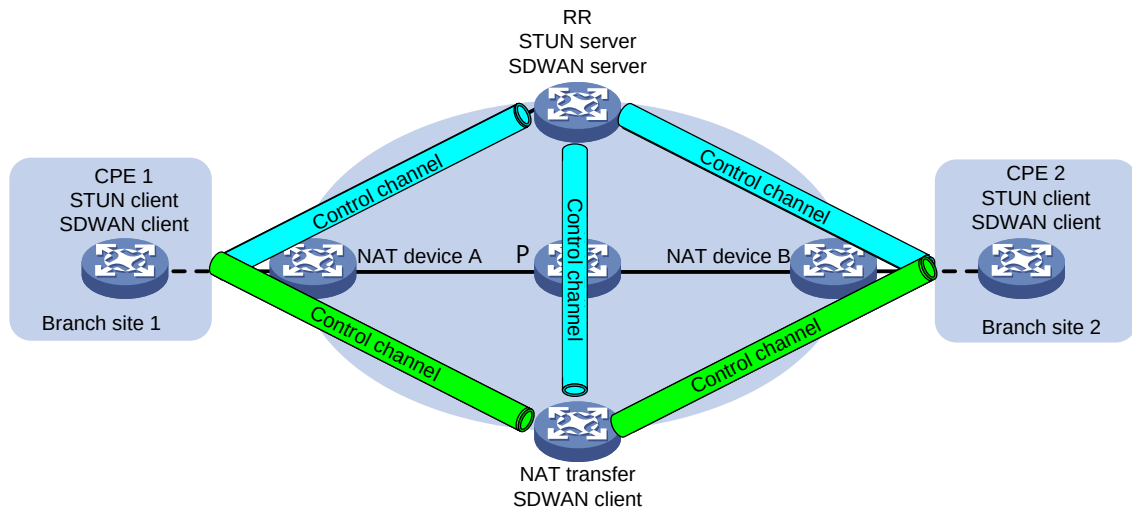
After a CPE (STUN client) obtains its public IP address and port number translated after NAT, it uses this public IP address to establish an SDWAN tunnel with the other CPE. If two CPEs cannot establish a direct data channel between them, you must deploy a NAT transfer on the transport network for the CPEs to communicate with each other.

Figure 16 SDWAN tunnel establishment with NAT traversal



This following information uses [Figure 17](#) to illustrate the control channel and data channel establishment processes.

**Figure 17 SDWAN tunnel establishment with NAT traversal
(deployed with a NAT transfer)**



Control channel establishment

As shown in [Figure 17](#), control channels are established in the following process:

1. The STUN clients and STUN server exchange STUN protocol packets. Each STUN client obtains the local NAT type, public IP address (public IP address translated after NAT when the STUN client accesses the STUN server), and port number.
2. The SDWAN clients and SDWAN server establish SSL connections. Then, they exchange TTE information, including the NAT type and public IP addresses obtained through STUN.
3. When CPE 1, CPE 2, and the NAT transfer receive TTE information from the RR, they compare the routing domain in the TTE information with the routing domain in the local TTE information. If the routing domains are the same one, they establish SDWAN tunnels destined for the RR. The destination IP address of the tunnels is the public IP address in the TTE information of the RR. If the routing domains are different, they do not establish SDWAN tunnels.
4. When the RR receives TTE information from CPE 1, CPE 2, and the NAT transfer, it compares the routing domain in the TTE information with the routing domain in the local TTE information. If the routing domains are the same one, the RR establishes SDWAN tunnels separately to CPE 1, CPE 2, and the NAT transfer.

If the NAT transfer belongs to the public network, the RR establishes an SDWAN tunnel destined for the public IP address of the NAT transfer. The public IP address is the public IP address in the TTE information of the NAT transfer.

If the NAT type in the TTE information of CPE 1 and CPE 2 is full cone NAT, the RR establishes SDWAN tunnels destined for the public IP addresses of the CPEs. The public IP addresses are the public IP addresses in the TTE information of the CPEs.

If the NAT type in the TTE information of CPE 1 and CPE 2 is port restricted full cone NAT, restricted full cone NAT, or symmetric NAT, the RR cannot access CPE 1 or CPE 2 through the public IP addresses of the CPEs in the TTE information. The RR cannot establish SDWAN tunnels to the CPEs according to the currently obtained TTE information. To establish SDWAN tunnels from the RR to the CPEs:

- a. CPE 1 and CPE 2 periodically send SDWAN control packets to the RR through the SDWAN tunnels established from the CPEs to the RR.
- b. The RR uses the outer source IP addresses of the received SDWAN control packets as the public IP addresses of the CPEs. The RR establishes SDWAN tunnels destined for the public IP addresses.

5. After SDWAN tunnel establishment, CPE 1, CPE 2, the NAT transfer, and the RR add user network routes (UNRs) destined for the system IP addresses of peer devices.
6. CPE 1, CPE 2, the NAT transfer, and the RR establish BGP connections (control channels) under the IPv4 tunnel-encap-ext address family based on the system IP addresses.

Data channel establishment

As shown in [Figure 17](#), data channels are established in the following process:

1. After CPE 1, CPE 2, the NAT transfer, and the RR establish BGP connections (control channels), CPE 1, CPE 2, and the NAT transfer advertise TTE information to the RR through IPv4 tunnel-encap-ext routes. The RR reflects the TTE information to its BGP neighbors.
2. The CPEs compare their NAT types to determine whether they can establish direct data channels. Table 41 shows the data channel compatibility for different NAT types.
 - If the CPEs can establish a direct data channel, the establishment procedure is the same as step 4 in "[Control channel establishment](#)."
 - If the CPEs cannot establish a direct data channel, you must deploy a NAT transfer in the network. The CPEs each establish a data channel to the NAT transfer. Inter-CPE data is first forwarded to the NAT transfer through a data channel. Then, the NAT transfer forwards the data to the destination CPE through the other data channel. The procedure for establishing a data channel between a CPE and a NAT transfer is the same as that for establishing an SDWAN tunnel between a CPE and an RR. For more information, see step 4 in "[Control channel establishment](#)."

Table 41 Data channel compatibility for different NAT types

CPE 1 NAT type	CPE 2 NAT type	Support for CPE-CPE direct tunnels	NAT transfer required for CPE intercommunication
Non-NAT	Full cone NAT	√	×
Non-NAT	Port restricted full cone NAT or restricted full cone NAT	√	×
Non-NAT	Symmetric NAT	√	×
Non-NAT	Unknown type	√	×
Non-NAT	Static NAT	√	×
Full cone NAT	Full cone NAT	√	×
Full cone NAT	Port restricted full cone NAT or restricted full cone NAT	√	×
Full cone NAT	Symmetric NAT	√	×
Full cone NAT	Unknown type	√	×
Full cone NAT	Static NAT	√	×
Port restricted full cone NAT or restricted full cone NAT	Port restricted full cone NAT or restricted full cone NAT	√	×
Port restricted full cone NAT or	Symmetric NAT	×	√

CPE 1 NAT type	CPE 2 NAT type	Support for CPE-CPE direct tunnels	NAT transfer required for CPE intercommunication
restricted full cone NAT			
Port restricted full cone NAT or restricted full cone NAT	Unknown type	×	√
Port restricted full cone NAT or restricted full cone NAT	Static NAT	√	×
Symmetric NAT	Symmetric NAT	×	√
Symmetric NAT	Unknown type	×	√
Symmetric NAT	Static NAT	√	×
Unknown type	Unknown type	×	√

SDWAN tasks at a glance

To configure SDWAN, perform the following tasks:

1. [Configuring site and device identification information](#)
 - a. [Specifying a site for the device](#)
 - b. [Specifying an ID and system IPv4 address for the device](#)
2. [Configuring an SDWAN client](#)
3. [Configuring an SDWAN server](#)
4. (Optional.) [Configuring IPsec-protected SDWAN tunnels](#)
For more information, see IPsec in *Security Configuration Guide*.
5. (Optional.) [Configuring SDWAN tunnels with NAT traversal](#)
For more information, see NAT in *Layer 3—IP Services Configuration Guide*.
6. [Configuring an SDWAN tunnel](#)
7. [Testing TTE connection connectivity](#)
8. [Configuring BGP to advertise IPv4 tunnel-encap-ext routes](#)
9. [Using BGP EVPN IP prefix advertisement routes to advertise routes for a VPN instance](#)
 - o [Configuring a CPE](#)
 - o [Configuring an RR](#)
 - o (Optional.) [Configuring traffic rerouting and load balancing by using the Priority-Color attribute](#)
 - o (Optional.) [Configuring next hop recursion based on only the Priority-Color attribute for IP prefix advertisement routes](#)
10. [Configuring SDWAN network intercommunication over an EVPN VXLAN network](#)
11. [Configuring SDWAN network intercommunication with an EVPN L3VPN over SRv6 network](#)
12. (Optional.) [Specifying the post-NAT public IP address and port number for tunneled packets](#)
13. (Optional.) [New feature: Simplifying the QoS configuration in a hub-spoke network](#)
14. [Simplifying the QoS configuration in a hub-spoke network](#)

Configuring site and device identification information

Specifying a site for the device

About this task

A site ID uniquely identifies a site in an SDWAN network.

You can specify a site name for a site to describe the site location and function to better identify the site in the SDWAN network. A site name does not uniquely identify a site. You can specify the same name for multiple devices.

Restrictions and guidelines

Different site roles have different functions. A site role change will cause SDWAN tunnel flapping and interrupt ongoing services. As a best practice, complete role configuration before the SDWAN network runs services.

Procedure

1. Enter system view.
system-view
2. Specify the ID of the site to which the device belongs.
sdwan site-id site-id
By default, no site ID is specified for the device.
3. Specify the name of the site to which the device belongs.
sdwan site-name site-name
By default, no site name is specified for the device.
4. Specify the role of the site to which the device belongs.
sdwan site-role { cpe | nat-transfer | rr } *
By default, no site role is specified for the device.
All SDWAN devices at the same site must be assigned the same site role.

Specifying an ID and system IPv4 address for the device

About this task

A device ID uniquely identifies a device at a site.

The device uses the system IPv4 address to set up BGP sessions with other devices. In an RIR scenario, the system IPv4 address is also used as the inner destination IPv4 address of probe packets sent by the NQA client in NQA link connectivity probes. For more information about RIR, see *Layer 3—IP Routing Configuration Guide*.

Procedure

1. Enter system view.
system-view
2. Assign an ID to the device.
sdwan device-id device-id
By default, no ID is assigned to the device.
3. Specify a system IPv4 address for the device.

sdwan system-ip *interface-type interface-number*

By default, no system IPv4 address is specified for the device.

The system IPv4 address must be unique in the SDWAN network.

For this command to take effect, you must specify a loopback interface that has an IPv4 address.

Configuring an SDWAN client

About this task

In an SDWAN network, the CPEs, NAT transfer, and RRs exchange TTE information through SSL connections. The CPEs and NAT transfer act as SDWAN clients and the RRs act as SDWAN servers.

Perform this task to specify an SSL client policy on a CPE or NAT transfer for the CPE or NAT transfer to establish SSL connections with RRs. After SSL connection establishment, the CPE or NAT transfer advertises its local TTE information to RRs. The RRs advertise their local TTE information to the CPE or NAT transfer. After TTE information exchange, the CPE or NAT transfer can establish SDWAN tunnels to the RRs.

Restrictions and guidelines

Only one SSL client policy can be applied to an SSL connection. If you execute the **sdwan ssl-client-policy** command multiple times, the most recent configuration takes effect and it takes effect only on SSL connections established after the modification.

Prerequisites

Complete the SSL client policy settings. For more information about SSL client policies, see SSL configuration in *Security Configuration Guide*.

Procedure

1. Enter system view.

system-view

2. Specify an SDWAN server on the CPE or NAT transfer.

sdwan server system-ip *system-ip-address* { **ip** *ipv4-address* | **ipv6** *ipv6-address* }
[**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

By default, no SDWAN servers are specified on a CPE or NAT transfer.

3. Specify an SSL client policy on the CPE or NAT transfer for the CPE or NAT transfer to establish SSL connections with RRs (SDWAN servers).

sdwan ssl-client-policy *policy-name*

By default, no SSL client policy is specified on a CPE or NAT transfer for the CPE or NAT transfer to establish SSL connections with RRs (SDWAN servers).

Configuring an SDWAN server

About this task

Perform this task to allow an RR to establish SSL connections with CPEs or the NAT transfer and advertise its local TTE information to the CPEs or NAT transfer. The CPEs or NAT transfer also advertise their local TTE information to the RR through the SSL connections. After TTE information exchange, the RR and the CPEs or NAT transfer will establish SDWAN tunnels based on the TTE information.

The device supports the following modes for SSL connection establishment:

- **Simple mode**—To use this mode, you do not need to specify an SSL server policy on the RR. The RR uses the self-signed certificate and the default settings of the SSL parameters to establish SSL connections with the CPEs or NAT transfer. The configuration for this mode is simple, but this mode is less secure than the secure mode.
- **Secure mode**—To use this mode, you must specify an SSL server policy on the RR and configure PKI domain settings. The configuration for this mode is complex, but this mode is more secure than the simple mode.

Restrictions and guidelines

Only one SSL server policy can be applied to an SSL connection. If you execute the **sdwan ssl-server-policy** command multiple times, the most recent configuration cannot take effect automatically. For the configuration to take effect, you must execute the **undo sdwan server enable** command and then the **sdwan server enable** command to re-enable the SDWAN server.

Prerequisites

To use the secure mode, first complete the SSL server policy settings. For more information about SSL server policies, see SSL configuration in *Security Configuration Guide*.

Procedure

1. Enter system view.
system-view
2. Enable SDWAN server on the RR.
sdwan server enable
By default, SDWAN server is disabled on an RR.
3. Specify a TCP port number for the SDWAN server on the RR.
sdwan server port port-number
By default, the TCP port number of the SDWAN server is 2004.
4. (Optional.) Specify an SSL server policy on the RR for the RR to establish SSL connections with CPEs or the NAT transfer (SDWAN clients).
sdwan ssl-server-policy policy-name
By default, no SSL server policy is specified on an RR for the RR to establish SSL connections with CPEs or the NAT transfer.

Configuring an SDWAN tunnel

About this task

After one CPE exchanges TTE information with another CPE or an RR, it compares the local TTE information with the received TTE information to determine whether to establish an SDWAN tunnel with the latter device.

- If they have the same routing domain, group ID, and transport network, they establish an SDWAN tunnel between them.
- If they have different routing domains, group IDs, or transport networks, they cannot establish an SDWAN tunnel.

Restrictions and guidelines

For information about tunnel configuration and tunnel interface commands, see tunneling in *Layer 3—IP Services Configuration Guide*.

You can specify a source UDP port number for SDWAN tunneled packets both in system view and in tunnel interface view.

- The source UDP port number specified in system view applies to all SDWAN tunnel interfaces.

- The source UDP port number specified in tunnel interface view applies only to a tunnel interface.

For a tunnel interface, the source UDP port number specified in tunnel interface view takes precedence over that specified in system view. If no source UDP port number is specified in tunnel interface view, the source UDP port number specified in system view applies.

Procedure

1. Enter system view.

system-view

2. (Optional.) Specify a global source UDP port number for SDWAN tunneled packets.

sdwan encapsulation global-udp-port *port-number*

By default, the global source UDP port number for SDWAN tunneled packets is 4799.

3. Create an SDWAN tunnel interface in UDP encapsulation mode and enter tunnel interface view.

interface tunnel *tunnel-number* **mode sdwan udp** [**ipv6**]

For packet tunneling to succeed, the two ends of a tunnel must use the same tunnel mode.

4. Specify a physical output interface for SDWAN tunneled packets.

tunnel out-interface *out-interface-type out-interface-number*

By default, no output interface is specified for tunneled packets. If ECMP routes exist, the device randomly selects an output interface to forward tunneled packets.

5. Assign an interface ID to the SDWAN tunnel interface.

sdwan interface-id *interface-id*

By default, no interface ID is assigned to an SDWAN tunnel interface.

6. (Optional.) Specify a source UDP port number for SDWAN tunneled packets.

sdwan encapsulation udp-port *port-number* [**dynamic** [*time*]]

By default, the source UDP port number of SDWAN tunneled packets is the global source UDP port number for SDWAN tunneled packets.

7. Specify a routing domain for the SDWAN tunnel.

sdwan routing-domain *domain-name* **id** *domain-id*

By default, no routing domain is specified for an SDWAN tunnel.

8. (Optional.) Specify a group ID for the SDWAN tunnel.

sdwan group-id *group-id*

By default, no group ID is specified for an SDWAN tunnel.

9. Specify a transport network for the SDWAN tunnel.

sdwan transport-network *network-name* **id** *network-id* [**restrict**]

By default, no transport network is specified for an SDWAN tunnel.

10. Specify a source IP address for the SDWAN tunnel. Choose one of the following options:

- Specify a source IP address for the tunnel.

source { *ipv4-address* | *ipv6-address* }

The specified IP address is used as the source address of SDWAN tunneled packets.

- Specify a source interface to provide source IP address for the tunnel.

source *interface-type interface-number*

The IP address of the specified interface is used as the source IP address of SDWAN tunneled packets.

By default, no source IP address is configured for an SDWAN tunnel.

Testing TTE connection connectivity

About testing TTE connection connectivity

Use BFD or keepalive to test the connectivity of TTE connections on an SDWAN tunnel. When a TTE connection fails, the device can quickly detect the failure and handle the failure issue accordingly, for example, switch the traffic on the TTE connection to other TTE connections.

When BFD is used, the local device periodically sends BFD control packets to the remote device over all TTE connections on an SDWAN tunnel. If the device does not receive any BFD control packets from the remote device over a TTE connection within the detection period, it determines that the TTE connection is unreachable to the remote device. For more information about BFD, see *High Availability Configuration Guide*.

When keepalive is used, the local device sends keepalive requests to the remote device over all TTE connections on an SDWAN tunnel at the specified keepalive interval.

- If the local device receives a keepalive response from the remote device over a TTE connection within a keepalive interval, it determines that the TTE connection is reachable to the remote device.
- If the local device cannot receive a keepalive response from the remote device on a TTE connection within a keepalive interval, it resends a keepalive request. If the local device still cannot receive a response within the keepalive interval multiplied by the maximum keepalive attempts, it determines that the TTE connection is unreachable to the remote device. The device no longer forwards packets through the TTE connection.

Restrictions and guidelines for testing TTE connection connectivity

If BFD is used to test the connectivity of TTE connections on an SDWAN tunnel, you must use the **sdwan bfd enable** command at both ends of the SDWAN tunnel.

If the **sdwan bfd enable** command is used on an SDWAN tunnel interface, the device determines the connectivity of TTE connections on that SDWAN tunnel based on the BFD detection result. If this command is not used on an SDWAN tunnel interface, the device determines the connectivity of TTE connections on that SDWAN tunnel based on the keepalive result.

Using BFD to test TTE connection connectivity

1. Enter system view.
system-view
2. Create an SDWAN tunnel interface in UDP encapsulation mode and enter tunnel interface view.
interface tunnel *tunnel-number* [mode sdwan udp [ipv6]]
3. Configure the device to use BFD to test the connectivity of TTE connections on the SDWAN tunnel.
sdwan bfd enable [template *template-name*]

By default, BFD is not used to test the connectivity of TTE connections on an SDWAN tunnel. The device uses keepalive packets to test the connectivity of TTE connections on an SDWAN tunnel.

Using keepalive to test TTE connection connectivity

1. Enter system view.
system-view
2. Create an SDWAN tunnel interface in UDP encapsulation mode and enter tunnel interface view.
interface tunnel *tunnel-number* [**mode sdwan udp** [**ipv6**]]
3. Configure keepalive for the SDWAN tunnel.
sdwan keepalive interval *interval* [**retry** *retries*]
By default, the keepalive interval is 10 seconds and the maximum number of keepalive attempts is 3.
In an RIR-SDWAN network, set the keepalive interval within the range of 1 to 5 seconds as a best practice.

Configuring BGP to advertise IPv4 tunnel-encap-ext routes

Restrictions and guidelines for BGP IPv4 tunnel-encap-ext route advertisement

For more information about BGP commands in this task, see *Layer 3—IP Routing Command Reference*.

Enabling BGP to advertise BGP IPv4 tunnel-encap-ext routes

1. Enter system view.
system-view
2. Enable a BGP instance and enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
By default, BGP is disabled and no BGP instances exist.
3. Specify a CPE or RR as a peer.
peer { *group-name* | *ipv4-address* [*mask-length*] } **as-number** *as-number*
4. Create the BGP IPv4 tunnel-encap-ext address family and enter BGP IPv4 tunnel-encap-ext address family view.
address-family ipv4 tnl-encap-ext
5. Enable BGP to exchange BGP IPv4 tunnel-encap-ext routes with a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **enable**
By default, BGP does not exchange BGP IPv4 tunnel-encap-ext routes with peers or peer groups.

Configuring BGP IPv4 tunnel-encap-ext route settings

Controlling BGP IPv4 tunnel-encap-ext route advertisement and reception

1. Enter system view.
system-view
2. Enter BGP instance view
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP IPv4 tunnel-encap-ext address family view.
address-family ipv4 tnl-encap-ext
4. Apply a routing policy to routes received from or advertised to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** *route-policy-name*
{ **export** | **import** }

By default, no routing policies are applied to routes received from or advertised to peers or peer groups.
5. Set the maximum number of routes that can be received from a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **route-limit** *prefix-number*
[{ **alert-only** | **discard** | **reconnect** *reconnect-time* } | *percentage-value*] *

By default, the number of routes that can be received from a peer or peer group is not limited.

Configuring BGP IPv4 tunnel-encap-ext route attributes

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP IPv4 tunnel-encap-ext address family view.
address-family ipv4 tnl-encap-ext
4. Set the local router as the next hop for routes advertised to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-local**

The default settings are as follows:
 - BGP sets the local router as the next hop for all routes advertised to an EBGp peer or peer group.
 - BGP does not set the local router as the next hop for EBGp routes advertised to an IBGP peer or peer group.
5. Set a preferred value for routes received from a peer or peer group
peer { *group-name* | *ipv4-address* [*mask-length*] } **preferred-value** *value*

By default, the preferred value is 0 for routes received from a peer or peer group.
6. Permit the local AS number to appear in routes from a peer or peer group and set the number of appearances.
peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop** [*number*]

By default, the local AS number is not allowed in routes from peers.

Configuring BGP route reflection

1. Enter system view.
system-view
2. Enter BGP instance view.

- bgp** *as-number* [**instance** *instance-name*]
3. Enter BGP IPv4 tunnel-encap-ext address family view.
address-family ipv4 tnl-encap-ext
 4. Configure the device as an RR and specify a CPE or NAT device as its client.
peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**
By default, no RR or clients are configured.
 5. (Optional.) Enable BGP IPv4 tunnel-encap-ext route reflection between clients.
reflect between-clients
By default, BGP IPv4 tunnel-encap-ext route reflection between clients is enabled.
 6. (Optional.) Configure the cluster ID of the RR.
reflector cluster-id { *cluster-id* | *ipv4-address* }
By default, an RR uses its own router ID as the cluster ID.

Configuring community attributes

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP IPv4 tunnel-encap-ext address family view.
address-family ipv4 tnl-encap-ext
4. Advertise the COMMUNITY attribute to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**
By default, the device does not advertise the COMMUNITY attribute to peers or peer groups.
5. Advertise the extended community attribute to a peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-ext-community**
By default, no extended community attribute is advertised to any peers or peer groups.

Maintaining BGP sessions

Perform the following tasks in user view:

- Reset BGP sessions of the BGP IPv4 tunnel-encap-ext address family.
reset bgp [**instance** *instance-name*] { *as-number* | *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **ipv4 tnl-encap-ext**
- Soft-reset BGP sessions of the BGP IPv4 tunnel-encap-ext address family.
refresh bgp [**instance** *instance-name*] { *ipv4-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **ipv4 tnl-encap-ext**

Using BGP EVPN IP prefix advertisement routes to advertise routes for a VPN instance

Configuring a CPE

About this task

In an SDWAN network, CPEs use BGP EVPN IP prefix advertisement routes to advertise site VPN routes. You must configure the CPEs to advertise BGP EVPN routes in SDWAN encapsulation.

If multiple VPN instances are deployed in the SDWAN network, you must perform the following tasks on the CPEs for each VPN instance:

- In VPN instance IPv4 or IPv6 address family view, enable EVPN to advertise SDWAN routes. This feature advertises VPN routes in the routing table of the VPN instance as BGP EVPN IP prefix advertisement routes in SDWAN encapsulation.
- In VPN instance view, specify a VN ID for the VPN instance. When VPN routes are advertised as IP prefix advertisement routes, the routes include the VN ID of the VPN instance. The VN ID is used to differentiate packets of different VPN instances.
- In BGP EVPN address family view, configure the device to advertise EVPN routes in SDWAN encapsulation to an RR.

Restrictions and guidelines

On a CPE, use the **evpn sdwan routing-enable** command in conjunction with the **peer advertise encap-type sdwan** command for a VPN instance. If you do not use both of the commands, the CPE cannot advertise the routes of the VPN instance to an RR.

Procedure

1. Enter system view.
system-view
2. Enter VPN instance view.
ip vpn-instance *vpn-instance-name*
3. Specify a VN ID for the VPN instance.
sdwan vn-id *vn-id*
By default, the VN ID of a VPN instance is 0.
4. Enter VPN instance IPv4 address family view or VPN instance IPv6 address family view.
 - Enter VPN instance IPv4 address family view.
address-family ipv4
 - Enter VPN instance IPv6 address family view.
address-family ipv6
5. Enable EVPN to advertise SDWAN routes.
evpn sdwan routing-enable
By default, EVPN cannot advertise SDWAN routes.
6. Return to system view.
quit
quit
7. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]

8. Enter BGP EVPN address family view.
address-family l2vpn evpn
9. Configure the device to advertise BGP EVPN routes in SDWAN encapsulation to an RR.
peer { group name | ipv4-address [mask-length] } advertise encap-type sdwan
By default, the device does not advertise BGP EVPN routes in SDWAN encapsulation to an RR.

Configuring an RR

About this task

In an SDWAN network, an RR reflects site VPN routes among CPEs. You must enable the RR to advertise BGP EVPN routes in SDWAN encapsulation to the CPEs.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP EVPN address family view.
address-family l2vpn evpn
4. Configure BGP route reflection:
 - a. Configure the device as an RR and specify the CPEs as its clients.
peer { group-name | ipv4-address [mask-length] } reflect-client
By default, no RR or clients are configured.
 - b. (Optional.) Enable BGP EVPN route reflection between clients.
reflect between-clients
By default, BGP EVPN route reflection between clients is enabled.
 - c. (Optional.) Configure the cluster ID of the RR.
reflector cluster-id { cluster-id | ipv4-address }
By default, an RR uses its own router ID as the cluster ID.
 - d. (Optional.) Create a reflection policy for the RR to filter reflected BGP EVPN routes.
rr-filter ext-comm-list-number
By default, an RR does not filter reflected BGP EVPN routes.
 - e. (Optional.) Enable the RR to change the attributes of routes to be reflected.
reflect change-path-attribute
By default, an RR cannot change the attributes of routes to be reflected.
5. Configure the device to advertise BGP EVPN routes in SDWAN encapsulation to a CPE.
peer { group name | ipv4-address [mask-length] } advertise encap-type sdwan
By default, the device does not advertise BGP EVPN routes in SDWAN encapsulation to a CPE.

Configuring traffic rerouting and load balancing by using the Priority-Color attribute

About the Priority-Color attribute

The Priority-Color attribute is a BGP extended community attribute. It is used only in SDWAN-encapsulated EVPN routes. In an SDWAN network, you can add backup routes for an EVPN route by adding the Priority-Color extended community attribute. Thus, when the data channel fails, traffic can bypass the data channel.

The Priority-Color extended community attribute is the format of *Priority:Site ID:Device ID* or *Priority:Site ID*. The value of priority determines the priority of the backup path, the smaller the value, the higher the priority. The site ID and device ID identify one or multiple bypass sites (SDWAN devices).

Working mechanism of the Priority-Color attribute

If an IP prefix advertisement route does not contain a Priority-Color attribute, only one route can be added to the BGP-VPN instance routing table or the VPN instance IP routing table. The route's next hop is the next hop of the IP prefix advertisement route. If the next hop is not reachable, the IP prefix advertisement route fails, and thus traffic forwarding to the IP prefix fails.

If an IP prefix advertisement route contains Priority-Color attributes, the device can add one primary route and multiple backup routes to the BGP-VPN instance routing table. If the Priority-Color attributes contain device IDs, the device generates a backup route based on each Priority-Color attribute. If the Priority-Color attributes do not contain device IDs, the device generates a backup route based on each SDWAN device in the site identified by the site ID in each Priority-Color attribute. The primary and backup routes use the same prefix. When a backup route is added to the VPN instance IP routing table, the next hop is the system IP of the device identified by the site ID and device ID in the Priority-Color attribute.

When the primary route is reachable, the primary route is added to the VPN instance IP routing table. When the primary route fails, the optimal backup route is added to the VPN instance IP routing table. The optimal backup route is determined as follows:

1. The backup route with the highest priority is the optimal backup route. The priority of a backup route is determined by the priority value in the Priority-Color attribute that generated the backup route, the smaller the priority value, the higher the priority.
2. If multiple backup routes have the same priority, the backup route with the lowest next hop IP address is the optimal route.

In BGP-VPN IPv4 or IPv6 unicast address family, if BGP load balancing is enabled by using the **balance** command, all optimal backup routes with the same priority are added to the VPN instance IP routing table for load balancing, regardless of the primary route's state.

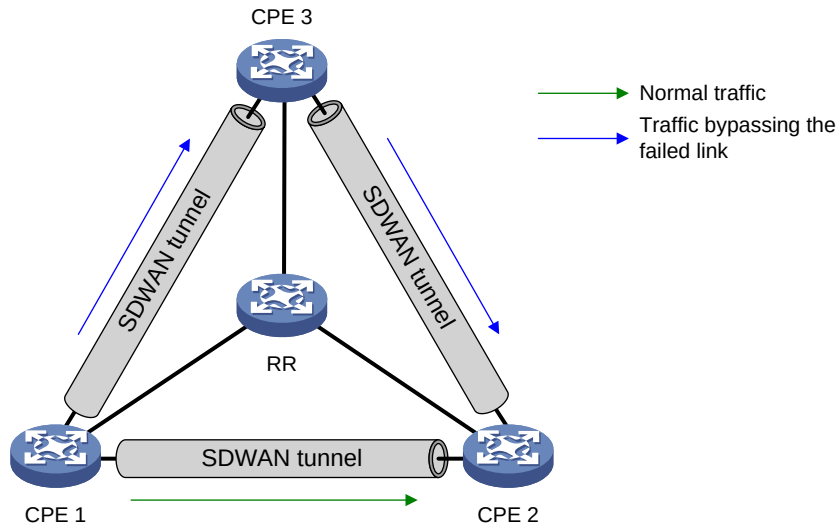
In BGP load balancing, the priority value of the primary route is regarded as 0. The primary route and the backup routes with priority value of 0 are all added to the VPN instance IP routing table for load balancing. When the primary route fails, the primary route does not participate in load balancing any longer. If no backup routes with priority value of 0 exist, only the primary route is added to the VPN instance IP routing table and no load balancing can be performed. After the primary route fails, all backup routes with the same, smallest priority value are added to the VPN instance IP routing table for load balancing.

For more information about BGP load balancing, see BGP configuration in *Layer 3—IP Routing Configuration Guide*.

Priority-Color attribute application

In an SDWAN network as shown in [Figure 18](#), an RR reflects BGP routes among CPE 1, CPE 2, and CPE 3. SDWAN tunnels are established between CPEs.

Figure 18 Priority-Color attribute application diagram



CPE 2 advertises the IP prefix routes of the local site to the RR. When reflecting the routes to CPE 1, the RR can use a routing policy to add Priority-Color attributes to EVPN routes. The site ID and device ID in the Priority-Color attribute are those of CPE 3 (the bypass site). After CPE 1 receives these IP prefix advertisement routes, it adds the routes to the BGP-VPN instance routing table and generates a primary route and a backup route for each of the IP prefixes:

- The primary route recurses to the SDWAN tunnel between CPE 1 and CPE 2.
- The backup route recurses to the SDWAN tunnel between CPE 1 and CPE 3.

When the link between CPE 1 and CPE 2 is normal, CPE 1 adds the primary route to the VPN instance IP routing table. After CPE 1 receives the traffic destined for the site of CPE 2, CPE 1 recurses the traffic to the SDWAN tunnel between CPE 1 and CPE 2.

When the link between CPE 1 and CPE 2 fails, the primary route fails as a result. CPE 1 adds the backup route to the VPN instance IP routing table. After CPE 1 receives the traffic destined for the site of CPE 2, CPE 1 recurses the traffic to the SDWAN tunnel between CPE 1 and CPE 3. CPE 3 then forwards the traffic to CPE 2. In this way, the traffic bypasses the failed link.

To use the links attached to CPE 3 to forward the traffic between CPE 1 and CPE 2 for load balancing, you can perform the following tasks:

- On the RR, set the priority value of the Priority-Color attribute to 0.
- On CPE 1, set the number of BGP routes for load balancing to a number equal to or greater than 2.

When CPE 1 receives traffic destined for the site attached to CPE 2, it forwards the traffic to both the SDWAN tunnels connected to CPE 2 and CPE 3 for load balancing.

Restrictions and guidelines

To use the Priority-Color extended community attribute for load balancing, you must use the **balance** command in BGP-VPN IPv4 unicast address family view or BGP-VPN IPv6 unicast address family view on CPEs. For more information about the **balance** command, see BGP commands in *Layer 3—IP Routing Command Reference*.

Procedure (RR)

1. Enter system view.
system-view
2. Create a routing policy and a node and enter routing policy node view.
route-policy route-policy-name { deny | permit } node node-number
3. (Optional.) Configure if-match clauses.

For more information about if-match clauses, see routing policy configuration in *Layer 3—IP Routing Configuration Guide*.

4. Configure Priority-Color extended community attributes for BGP routes.

apply extcommunity priority-color *priority-color*<1–32> [**additive**]

By default, no Priority-Color extended community attributes are configured for BGP routes.

5. Return to system view.

quit

6. Enter BGP instance view.

bgp *as-number* [**instance** *instance-name*]

7. Enter BGP EVPN address family view.

address-family *l2vpn evpn*

8. Apply the routing policy to add the Priority-Color extended community attributes to the EVPN routes for a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
route-policy *route-policy-name* { **export** | **import** }

By default, no routing policy is applied to a peer or peer group.

Configuring next hop recursion based on only the Priority-Color attribute for IP prefix advertisement routes

About this task

By default, the device performs next hop recursion for IP prefix advertisement routes based on both the NEXT_HOP and Priority-Color attributes after it receives these routes if these routes have the Priority-Color attribute. The next hop recursion procedure is as follows for an IP prefix advertisement route:

- Typically, the address in the NEXT_HOP attribute is the system IP address of a remote CPE. The device looks up for a matching TTE connection based on the address. The SDWAN tunnel interface of the matching TTE connection is the next hop output interface obtained through next hop recursion for the IP prefix advertisement route.
- Each Priority-Color attribute includes the site ID information of a remote CPE or the site ID and device ID information of a remote CPE. The device looks up for matching TTE connections based on the information. The SDWAN tunnel interfaces of the matching TTE connections are the next hop output interfaces obtained through next hop recursion for the IP prefix advertisement route based on the Priority-Color attributes.

When the device receives packets that match an IP prefix advertisement route, it forwards the packets as follows:

- If BGP load balancing is not configured, the device forwards the packets over an SDWAN tunnel obtained through next hop recursion based on the NEXT_HOP attribute of the IP prefix advertisement route. When that SDWAN tunnel is not available, the device uses the SDWAN tunnel obtained through next hop recursion based on the Priority-Color attribute to forward the packets.
- If BGP load balancing is configured, the device can forward the packets over the following SDWAN tunnels for load balancing:
 - The SDWAN tunnel obtained through next hop recursion based on the NEXT_HOP attribute of the IP prefix advertisement route.
 - The SDWAN tunnels obtained through next hop recursion based on the Priority-Color attributes of the IP prefix advertisement route.

The Priority-Color attribute is easy to configure, and the device can flexibly control the SDWAN forwarding path through this attribute. To perform next hop recursion for IP prefix advertisement

routes that have the Priority-Color attribute based on only the Priority-Color attribute, use the feature in this section. With this feature, when the device receives packets that match an IP prefix advertisement route, it forwards the packets to an SDWAN tunnel obtained through next hop recursion based on only the Priority-Color attribute. In this way, the forwarding path is not restricted by the NEXT_HOP attribute of the IP prefix advertisement route. To adjust the forwarding path, you only need to modify the Priority-Color attribute.

Restrictions and guidelines

This feature takes effect only on SDWAN-encapsulated IP prefix advertisement routes that have the Priority-Color attribute.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP EVPN address family view.
address-family l2vpn evpn
4. Configure next hop recursion based on only the Priority-Color attribute for SDWAN-encapsulated IP prefix advertisement routes.
evpn-sdwan nexthop-recursive priority-color-only

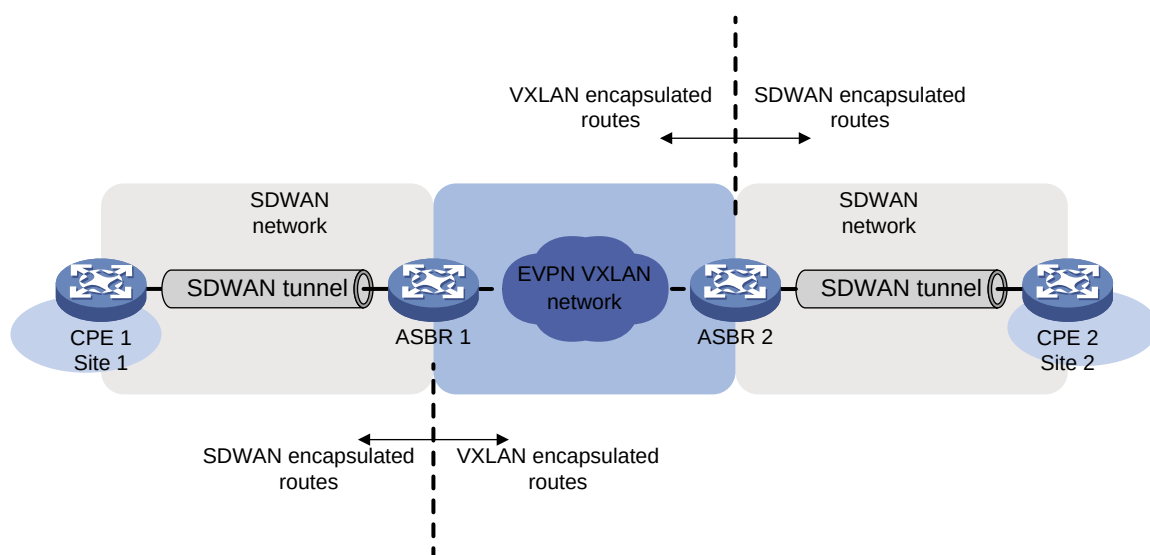
By default, the device performs next hop recursion first based on the NEXT_HOP attribute and then the Priority-Color attribute for an IP prefix advertisement route that has the Priority-Color attribute after it receives that route.

Configuring SDWAN network intercommunication over an EVPN VXLAN network

About this task

As shown in Figure 19, CPE 1 and CPE 2 belong to different SDWAN networks that are connected over an EVPN VXLAN network. ASBR 1 and ASBR 2 belong to the SDWAN networks and EVPN VXLAN network. Tenants at site 1 and site 2 communicate with one another over the EVPN VXLAN network.

Figure 19 Network diagram for SDWAN network intercommunication over an EVPN VXLAN network



For SDWAN networks to communicate with each other over an EVPN VXLAN network, use the **peer re-originated** command on the edge devices of the SDWAN networks, in this example, on ASBR 1 and ASBR 2. When this command is used, ASBR 1 and ASBR 2 process IP prefix advertisement routes as follows:

- When ASBR 1 or ASBR 2 receives an SDWAN-encapsulated IP prefix advertisement route, it performs the following operations to ensure that the route can be received and forwarded by a peer in the EVPN VXLAN network:
 - a. Replaces the next hop address of the route with the local address.
 - b. Converts the route into a VXLAN-encapsulated IP prefix advertisement route.
- When ASBR 1 or ASBR 2 receives a VXLAN-encapsulated IP prefix advertisement route, it performs the following operations to ensure that the route can be received and forwarded by a peer in the SDWAN network:
 - c. Replaces the next hop address of the route with the local address.
 - d. Converts the route into an SDWAN-encapsulated IP prefix advertisement route.

Private routes at one site attached to an SDWAN network can reach the remote site attached to the other SDWAN network over the SDWAN networks and EVPN VXLAN network, so that tenants at the sites can communicate with one another.

Restrictions and guidelines

The device advertises only reoriginated BGP routes received from a peer specified by using the **peer re-originated** command to other peers. As a result, when the device receives VXLAN-encapsulated IP prefix advertisement routes from the peer, it cannot advertise the routes to other peers in the EVPN VXLAN network. For the device to advertise both original and reoriginated BGP routes to peers or peer groups, execute the **peer advertise original-route** command on the device. For more information about the **peer advertise original-route** command, see SRv6 VPN commands in *Segment Routing Command Reference*.

Prerequisites

Complete EVPN VXLAN settings on the ASBRs to ensure that the ASBRs can exchange VXLAN-encapsulated BGP EVPN routes with BGP peers and perform Layer 2 and Layer 3 forwarding for VXLAN traffic. For more information about EVPN VXLAN configuration, see *EVPN Configuration Guide*.

Complete SDWAN settings on the ASBRs to ensure that the ASBRs can perform the following operations:

- Establish SDWAN tunnels with the RRs and CPEs in the same routing domain.
- Exchange BGP IPv4 tunnel-encap-ext routes with other SDWAN devices.
- Use SDWAN-encapsulated IP prefix advertisement routes to advertise VPN routes of the local site.

Procedure (ASBR)

1. Enter system view.

system-view

2. Enter BGP instance view.

bgp *as-number* [**instance** *instance-name*]

3. Enter BGP EVPN address family view.

address-family **l2vpn evpn**

4. Replace the L3 VXLAN ID, RD, and route targets (optional) of IP prefix advertisement routes received from an RR or EVPN VXLAN peer.

peer { *group-name* | *ipv4-address* [*mask-length*] } **re-originated** [**ip-prefix**]
[**replace-rt**]

By default, the device does not modify the BGP EVPN routes that are received from peers or peer groups.

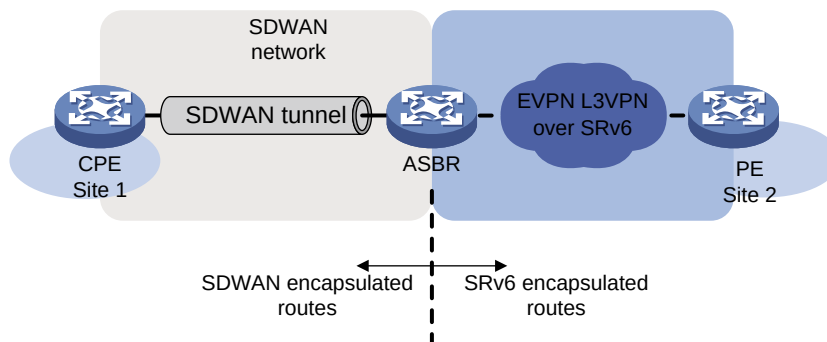
For more information about this command, see EVPN commands in *EVPN Command Reference*.

Configuring SDWAN network intercommunication with an EVPN L3VPN over SRv6 network

About this task

As shown in Figure 20, site 1 and site 2 must traverse an SDWAN network and an EVPN L3VPN over SRv6 network to communicate with each other. The CPE belongs to the SDWAN network. The ASBR belongs to both the SDWAN network and the EVPN L3VPN over SRv6 network. The PE belongs to the EVPN L3VPN over SRv6 network.

Figure 20 SDWAN network intercommunication with an EVPN L3VPN over SRv6 network



For the SDWAN network to communicate with the EVPN L3VPN over SRv6 network, use the **peer re-originated** command on the ASBR, the edge device of the SDWAN network. When this command is used, the ASBR processes IP prefix advertisement routes as follows:

- When the ASBR receives an SDWAN-encapsulated IP prefix advertisement route, it performs the following operations to ensure that the route can be received and forwarded by the PE in the EVPN L3VPN over SRv6 network:
 - a. Replaces the next hop address of the route with the local address.
 - b. Converts the route into an SRv6-encapsulated IP prefix advertisement route.
- When the ASBR receives an SRv6-encapsulated IP prefix advertisement route, it performs the following operations to ensure that the route can be received and forwarded by the CPE in the SDWAN network:
 - c. Replaces the next hop address of the route with the local address.
 - d. Converts the route into an SDWAN-encapsulated IP prefix advertisement route.

Private routes at site 1 can reach site 2 over the SDWAN network and the EVPN L3VPN over SRv6 network, so that tenants at the sites can communicate with one another.

Restrictions and guidelines

The device advertises only reoriginated BGP routes received from a peer specified by using the **peer re-originated** command to other peers. For the device to also advertise original BGP routes to peers or peer groups, execute the **peer advertise original-route** command on the device. For more information about the **peer advertise original-route** command, see SRv6 VPN commands in *Segment Routing Command Reference*.

On the ASBR, make sure the device learns the received SRv6-encapsulated and SDWAN-encapsulated IP prefix advertisement routes to the routing table of the same VPN instance.

For tenants to communicate with one another across an SDWAN network and an EVPN L3VPN over SRv6 network, make sure the tenants belong to the same VPN instance.

Prerequisites

Complete EVPN L3VPN over SRv6 settings on the ASBR to ensure that the ASBR can exchange SRv6-encapsulated BGP EVPN routes with the PE. For more information about EVPN L3VPN over SRv6 configuration, see *Segment Routing Configuration Guide*.

Complete SDWAN settings on the ASBR to ensure that the ASBR can perform the following operations:

- Establishes SDWAN tunnels with the RRs and CPEs in the same routing domain.
- Exchanges BGP IPv4 tunnel-encap-ext routes.
- Uses SDWAN-encapsulated IP prefix advertisement routes to advertise VPN routes of the local site.

Procedure (ASBR)

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP EVPN address family view.
address-family l2vpn evpn
4. Modify the encapsulation type and route information of the IP prefix advertisement routes received from a CPE or PE.
peer { group-name | ipv4-address [mask-length] } re-originated [ip-prefix] [replace-rt]

By default, the device does not modify the BGP EVPN routes that are received from peers or peer groups.

For more information about this command, see EVPN commands in *EVPN Command Reference*.

Specifying the post-NAT public IP address and port number for tunneled packets

About this task

Use this feature on a CPE or RR if the CPE or RR is behind a NAT device and the NAT device is configured with static NAT. With this feature, you do not need to configure STUN to detect the post-NAT public IP address and port number for the source IP address and port number of tunneled packets on the CPE or RR.

Restrictions and guidelines

Using this feature on a tunnel interface causes the device to disconnect all existing TTE connections established to the tunnel interface. The device will reestablish these TTE connections based on the specified post-NAT public IP address and port number.

As a best practice, do not configure this feature if the public network cannot actively access the internal network.

Procedure

1. Enter system view.

system-view

2. Create an IPv4 SDWAN tunnel interface in UDP encapsulation mode and enter tunnel interface view.

interface tunnel *tunnel-number* mode sdwan udp

For packet tunneling to succeed, the two ends of a tunnel must use the same tunnel mode.

3. Specify the post-NAT public IP address and port number for the source IP address and port number of tunneled packets.

sdwan nat-global-ip *global-address* global-port *global-port*

By default, the post-NAT public IP address and port number are not specified for the source IP address and port number of tunneled packets.

Simplifying the QoS configuration on a hub-spoke network

About this task

In the SDWAN scenario, a large number of spoke devices exist in a hub-spoke network. To configure a QoS policy for each hub-spoke SDWAN tunnel, you need to manually configure and apply a QoS policy on the hub device in the central site each time a spoke device is added for a branch site. If the QoS policies for the SDWAN tunnels from the central site to the branch sites are the same except for the rate limiting settings, you can simplify QoS policy configuration on the hub device by executing this task on the spoke devices.

After you execute this task on a spoke device, the spoke device will send a QoS TTE route to the peer hub device during hub-spoke data channel establishment. This route carries the user profile and traffic rate limit information specified in this task. Assume you specify a user profile on the spoke. The specified user profile will be advertised by BGP to the peer hub device along with the TTE information. The peer hub device will apply the local user profile that has the same name as the advertised user profile to the outbound direction of the hub-spoke SDWAN tunnel. If the user profile is not configured on the peer hub device or the user profile does not contain any configuration, the SDWAN tunnel will not be affected.

Restrictions and guidelines

If the user profile applied to the hub device has inbound QoS settings, those settings do not take effect on the SDWAN tunnel from the hub to the spoke. For example, the **qos car inbound** command configured in user profile view does not take effect on the hub-spoke SDWAN tunnel.

On the hub device, execute the **qos lr outbound** command with the **peer-advertise-bandwidth** keyword specified in the view of the user profile applied to the SDWAN tunnel. This configuration enables the hub device to accept the rate limit settings advertised from the peer spoke device. If you do not do so, the traffic rate limit specified by the **qos bandwidth downstream** command on the spoke device does not take effect on the hub device. For more information about the **qos lr outbound** command in user profile view, see QoS commands in *ACL and QoS Command Reference*.

Prerequisites

Before you perform this task, complete the following tasks on the hub device:

- Create the specified user profile.
- Configure QoS policy, traffic policing, traffic shaping, traffic rate limiting, or priority queue settings for the user profile as needed.

For more information about user profiles, see *Security Configuration Guide*.

Procedure

1. Enter system view.

system-view

2. Create a UDP-encapsulated SDWAN tunnel and enter tunnel interface view.

interface tunnel tunnel-number mode sdwan udp [ipv6]

Configure the same tunnel mode at both sides of a tunnel. Otherwise, the tunnel cannot transmit packets correctly.

3. Specify the user profile to be applied to the outbound direction of the peer tunnel interface.

qos apply user-profile profile-name downstream

By default, the user profile to be applied to the outbound direction of the peer tunnel interface is not specified. For more information about this command, see QoS commands in *ACL and QoS Command Reference*.

4. (Optional.) Set the traffic rate limit to be applied to the outbound direction of the peer tunnel interface.

qos bandwidth downstream bandwidth-value

By default, the traffic rate limit to be applied to the outbound direction of the peer tunnel interface is not set. For more information about this command, see QoS commands in *ACL and QoS Command Reference*.

Command reference

address-family ipv4 tnl-encap-ext

Use **address-family ipv4 tnl-encap-ext** to create the BGP IPv4 tunnel-encap-ext address family and enter BGP IPv4 tunnel-encap-ext address family view, or directly enter BGP IPv4 tunnel-encap-ext address family view if the BGP IPv4 tunnel-encap-ext address family already exists.

Use **undo address-family ipv4 tnl-encap-ext** to delete the BGP IPv4 tunnel-encap-ext address family and all settings in the address family.

Syntax

address-family ipv4 tnl-encap-ext

undo address-family ipv4 tnl-encap-ext

Default

The BGP IPv4 tunnel-encap-ext address family does not exist.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

Settings in BGP IPv4 tunnel-encap-ext address family view take effect only on routes in the BGP IPv4 tunnel-encap-ext address family.

Examples

In BGP instance view, create the BGP IPv4 tunnel-encap-ext address family and enter BGP IPv4 tunnel-encap-ext address family view.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] address-family ipv4 tnl-encap-ext
```

```
[Sysname-bgp-default-tnlencap-ipv4]
```

display bgp routing-table ipv4 tnl-encap-ext

Use **display bgp routing-table ipv4 tnl-encap-ext** to display information about BGP IPv4 tunnel-encap-ext routes.

Syntax

```
display bgp [ instance instance-name ] routing-table ipv4 tnl-encap-ext [ peer ipv4-address { advertised-routes | received-routes } [ statistics ] ] [ route-type { tte | tte-ipv6 | tte-qos | saas-path } ] [ { tnlencap-route route-length | tnlencap-prefix } [ advertise-info ] ] | statistics ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance *instance-name*: Specifies a BGP instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a BGP instance, this command displays information about BGP IPv4 tunnel-encap-ext routes in the default instance.

peer: Displays BGP IPv4 tunnel-encap-ext routes advertised to or received from a peer.

ipv4-address: Specifies the peer by its IPv4 address.

advertised-routes: Displays BGP IPv4 tunnel-encap-ext routes advertised to the specified peer.

received-routes: Displays BGP IPv4 tunnel-encap-ext routes received from the specified peer.

statistics: Displays BGP IPv4 tunnel-encap-ext route statistics.

route-type: Specifies a type of BGP IPv4 tunnel-encap-ext routes.

tte: Specifies IPv4 transport tunnel endpoint (TTE) advertisement routes.

tte-ipv6: Specifies IPv6 transport tunnel endpoint (TTE) advertisement routes.

tte-qos: Specifies QoS transport tunnel endpoint (TTE) advertisement routes.

saas-path: Specifies Software as a Service (SaaS) access path quality advertisement routes.

tnlencap-route: Displays detailed information about a BGP IPv4 tunnel-encap-ext route. The *tnlencap-route* argument is a string of 1 to 512 characters.

route-length: Specifies the length of the specified BGP IPv4 tunnel-encap-ext route, in bits. The value range is 0 to 65535.

tnlencap-prefix: Displays detailed information about a BGP IPv4 tunnel-encap-ext route. The *tnlencap-prefix* argument is a case-insensitive string of 1 to 512 characters. The string contains the route and route length in the format of *tnlencap-route/route-length*.

advertise-info: Displays advertisement information for BGP IPv4 tunnel-encap-ext routes.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all BGP IPv4 tunnel-encap-ext routes.

Examples

Display brief information about all BGP IPv4 tunnel-encap-ext routes.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext
```

```
BGP local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - dampened, h - history
```

```
              s - suppressed, S - stale, i - internal, e - external
```

```
              a - additional-path
```

```
Origin: i - IGP, e - EGP, ? - incomplete
```

```
Total number of routes: 2
```

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
* >i [1] [10] [10] [100] /40	2.2.2.2	0	100	0	i
* >i [3] [30] [30] [100] /40	2.2.2.2	0	100	0	i
* >i [2] [0x00ffffff] [abc] /552	2.2.2.2	0	100	0	i
* >i [4] [10] [10] [100] /40	2.2.2.2	0	100	0	i
* >i [5] [10] [10] [100] /40	127.0.0.1	0	100	0	i

Table 42 Command output

Field	Description
Status codes	Route state codes:

Field	Description
	• * – valid—Valid route. • > – best—Optimal route. • d - dampened—Dampened route. • h – history—History route. • s – suppressed—Suppressed route. • S – stale—Stale route. • i – internal—Internal route. • e – external—External route. • a – additional-path—Add-Path optimal route.
Origin	Origin of the route: • i – IGP—Originated in the current AS. • e – EGP—Learned through EGP. • ? – incomplete—Unknown origin.
Total number of routes	Total number of BGP IPv4 tunnel-encap-ext routes.
Network	BGP IPv4 tunnel-encap-ext route and route length. The following BGP IPv4 tunnel-encap-ext routes are supported: • [1] [SiteID][DeviceID][InterfaceID] ◦ 1—IPv4 TTE advertisement route. ◦ SiteID—Site ID. ◦ DeviceID—Device ID. ◦ InterfaceID—Interface ID. • [2][SiteAndDeviceID][SaaSName] ◦ 2—SaaS access path quality advertisement route. ◦ SiteAndDeviceID—Site ID and device ID of a SaaS cloud service. A SaaS cloud service connection is identified by the site ID and device ID of the SaaS cloud service. ◦ SaaSName—Name of the SaaS cloud service. • [3] [SiteID][DeviceID][InterfaceID] ◦ 3—IPv6 TTE advertisement route. ◦ SiteID—Site ID. ◦ DeviceID—Device ID. ◦ InterfaceID—Interface ID. • [4][SiteID][DeviceID][InterfaceID] ◦ 4—QoS TTE advertisement route. ◦ SiteID—Site ID. ◦ DeviceID—Device ID. ◦ InterfaceID—Interface ID. • [5][SiteID][DeviceID][InterfaceID] ◦ 5—RIR TTE advertisement route. ◦ SiteID—Site ID. ◦ DeviceID—Device ID. ◦ InterfaceID—Interface ID.
NextHop	Next hop IP address.
MED	Multi-exit discriminator (MED) attribute value.
LocPrf	Local preference value.
PrefVal	Preferred value.
Path/Ogn	AS_PATH and ORIGIN attributes of the route: • AS_PATH—Records the ASs the route has passed, which avoids routing loops. This field can display a maximum of 16 ASs. If the number of ASs exceeds the maximum number of ASs that can be displayed, an ellipsis

Field	Description
	(...) is displayed in place of the exceeding text. To view the complete information, display detailed information about the route.
	ORIGIN—Identifies the origin of the route.

Display detailed information about BGP IPv4 tunnel-encap-ext route [1][10][10][100]/40.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext [1][10][10][100]/40
```

```
BGP local router ID: 1.1.1.1
```

```
Local AS number: 100
```

```
Total number of routes: 1
```

```
Paths: 1 available, 1 best
```

```
BGP routing table information of [1][10][10][100]/40:
```

```
From : 4.4.4.4 (4.4.4.4)
```

```
Rely nexthop : 10.1.1.2
```

```
Original nexthop: 2.2.2.2
```

```
OutLabel : NULL
```

```
RxPathID : 0x0
```

```
TxPathID : 0x0
```

```
AS-path : 200
```

```
Origin : egp
```

```
Attribute value : MED 0, pref-val 0
```

```
State : valid, external, best
```

```
IP precedence : N/A
```

```
QoS local ID : N/A
```

```
Traffic index : N/A
```

```
Route type : Transport Tunnel Endpoint advertisement route
```

```
LinkID : 0x000a0a64
```

```
SiteID : 10
```

```
DeviceID : 10
```

```
InterfaceID : 100
```

```
SiteName : sdwan
```

```
SystemIP : 2.2.2.2
```

```
SiteRole : CPE
```

```
EncapType : UDP
```

```
EncapPort : 65535
```

```
SourceIP : 2.2.2.2
```

```
TNName : sdwan
```

```
TNID : 0x64
```

```
RDName : BGP
```

```
RDID : 0x64
```

```
IPSecEnable : Enabled
```

```
AH SA SPI : 0x0
```

```
ESP SA SPI : 0x0
```

```
ESPEncAlg : 0x1
```

```
ESPAuthAlg : 0x1
```

```
AHAuthAlg : 0x1
```

NATEnable : Enabled
NATType : Full Cone NAT
PublicAddress : 3.3.3.3
PublicPort : 179

Display detailed information about BGP IPv4 tunnel-encap-ext route [3][10][10][200]/40.

<Sysname> display bgp routing-table ipv4 tnl-encap-ext [3][10][10][200]/40

BGP local router ID: 50.50.50.50
Local AS number: 200

Paths: 1 available, 1 best

BGP routing table information of [3][10][10][200]/40:

From : 10.10.10.10 (50.50.50.10)
Rely nexthop : 0.0.0.0
Original nexthop: 10.10.10.10
OutLabel : NULL
RxPathID : 0x0
TxPathID : 0x0
AS-path : (null)
Origin : igp
Attribute value : MED 0, localpref 100, pref-val 0
State : valid, internal, best
IP precedence : N/A
QoS local ID : N/A
Traffic index : N/A
VPN-Peer UserID : N/A
DSCP : N/A
EXP : N/A
Route type : IPv6 transport tunnel endpoint advertisement route
LinkID : 0x000a0ac8
SiteID : 10
DeviceID : 10
InterfaceID : 200
SiteName : shanghai
SystemIP : 10.10.10.10
SiteRole : RR
EncapType : UDP IPv6
EncapPort : 4799
SourceIP : 14::1
TNName : tnrripv6
TNID : 0xc8
RDName : rdr
RDID : 0x64
IPSecEnable : Disabled
AH SA SPI : 0x0
ESP SA SPI : 0x0
ESPEncAlg : 0x0

ESPAuthAlg : 0x0
AHAuthAlg : 0x0
NATEnable : Disabled
NATType : -
PublicAddress :
PublicPort :

Display detailed information about BGP IPv4 tunnel-encap-ext route [4][10][10][200]/40.

<CPE4>display bgp routing-table ipv4 tnl-encap-ext [4][10][10][200]/40

BGP local router ID: 50.50.50.50
Local AS number: 200

Paths: 1 available, 1 best

BGP routing table information of [4][10][10][200]/40:

From : 10.10.10.10 (50.50.50.10)
Rely nexthop : 0.0.0.0
Original nexthop: 10.10.10.10
OutLabel : NULL
RxPathID : 0x0
TxPathID : 0x0
AS-path : (null)
Origin : igp
Attribute value : MED 0, localpref 100, pref-val 0
State : valid, internal, best
IP precedence : N/A
QoS local ID : N/A
Traffic index : N/A
VPN-Peer UserID : N/A
DSCP : N/A
EXP : N/A
Route type : Qos transport tunnel endpoint advertisement route
LinkID : 0x000a0ac8
QoS TTE info : BW:1000/PF:a

Display detailed information about BGP IPv4 tunnel-encap-ext route [5][40][40][70]/40.

<Sysname> display bgp routing-table ipv4 tnl-encap-ext [5][40][40][70]/40

BGP local router ID: 1.1.1.1
Local AS number: 100

Paths: 1 available, 1 best

BGP routing table information of [5][40][40][70]/40:

Imported route.
Original nexthop: 127.0.0.1
OutLabel : NULL
RxPathID : 0x0
TxPathID : 0x0

```

AS-path          : (null)
Origin           : igp
Attribute value  : MED 0, localpref 100, pref-val 32768
State            : valid, local, best
IP precedence    : N/A
QoS local ID     : N/A
Traffic index    : N/A
VPN-Peer UserID  : N/A
DSCP             : N/A
EXP             : N/A
Route type       : IPv4 transport tunnel endpoint advertisement route ext-local
LinkID           : 0x00282846
SiteID           : 40
DeviceID         : 40
InterfaceID      : 70
SystemIP         : 7.7.7.7

```

Table 43 Command output

Field	Description
Total number of routes	Total number of BGP IPv4 tunnel-encap-ext routes.
Paths	Number of routes: available—Number of valid routes. best—Number of optimal routes.
BGP routing table information of [1][10][10][100]/40	Detailed information about BGP IPv4 tunnel-encap-ext route [1][10][10][100]/40.
From	IP address of the BGP peer that advertised the route.
Rely Nexthop	Next hop IP address after route recursion. If no next hop IP address is found, this field displays not resolved .
Original nexthop	Original next hop address of the route. If the route was obtained from a BGP update message, the original next hop address is the next hop IP address in the message.
OutLabel	Outgoing label of the route. This field is not supported by the BGP IPv4 tunnel-encap-ext address family in the current software version.
RxPathID	Add-Path ID value of the received route. This field is not supported by the BGP IPv4 tunnel-encap-ext address family in the current software version.
TxPathID	Add-Path ID value of the sent route. This field is not supported by the BGP IPv4 tunnel-encap-ext address family in the current software version.
AS-path	AS_PATH attribute of the route. This attribute records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: igp—Originated in the current AS. egp—Learned through EGP. incomplete—Unknown origin.
Attribute value	BGP attributes of the route: MED—MED value for the destination network.

Field	Description
	• localpref—Local preference value. • pref-val—Preferred value. • pre—Protocol preference value.
State	Route state: • valid—Valid route. • internal—Internal route. • external—External route. • local—Local route. • best—Optimal route.
IP precedence	IP precedence of the route, in the range of 0 to 7. If the IP precedence is invalid, this field displays N/A .
QoS local ID	QoS local ID of the route, in the range of 1 to 4095. If the QoS local ID is invalid, this field displays N/A .
Traffic index	Traffic index in the range of 1 to 64. If the traffic index is invalid, this field displays N/A .
LinkID	Link ID assigned to the TTE. A link ID identifies a TTE connection.
QoS TTE info	QoS TTE information carried in the route: • BW—Traffic rate limit to be applied to the outbound direction of the SDWAN tunnel on the hub device. • PF—User profile to be applied to the outbound direction of the SDWAN tunnel on the hub device.
SiteID	Site ID.
DeviceID	Device ID.
InterfaceID	Interface ID.
SiteName	Site name.
SystemIP	Site system IP address.
SiteRole	Site role: • CPE. • RR. • NAT transfer. If multiple site roles are assigned, each two roles are separated by a slash (/). For example: CPE/RR/NAT transfer .
EncapType	Encapsulation mode, which can be only UDP in the current software version.
EncapPort	Local UDP port number for SDWAN encapsulation.
SourceIP	Source IP address of the tunnel.
TNName	Transport network name.
TNID	Transport network ID.
RDName	Routing domain name.
RDID	Routing domain ID.
IPSecEnable	IPsec state: • Enabled—IPsec protection is enabled. • Disabled—IPsec protection is disabled.

Field	Description
AH SA SPI	AH SA SPI.
ESP SA SPI	ESP SA SPI.
ESPEncAlg	ESP encryption algorithm.
ESPAuthAlg	ESP authentication algorithm.
AHAuthAlg	AH authentication algorithm.
NATEnable	Whether NAT is deployed: Enabled—NAT is deployed. Disabled—NAT is not deployed.
NATType	NAT type: Full Cone NAT. Restricted Cone NAT. Port Restricted Cone NAT. Symmetric NAT. If no NAT type exists, this field displays a hyphen (-).
PublicAddress	Public IP address after NAT.
PublicPort	Public port number after NAT.

Display detailed information about BGP IPv4 tunnel-encap-ext route [2][16777216][abc]/296.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext [2][0x00ffffff][abc]/296
```

```
BGP local router ID: 1.1.1.1
```

```
Local AS number: 100
```

```
Total number of routes: 1
```

```
Paths: 1 available, 1 best
```

```
BGP routing table information of [2][0x00ffffff][abc]/296:
```

```
From : 4.4.4.4 (4.4.4.4)
```

```
Rely nexthop : 10.1.1.2
```

```
Original nexthop: 2.2.2.2
```

```
OutLabel : NULL
```

```
RxPathID : 0x0
```

```
TxPathID : 0x0
```

```
AS-path : 200
```

```
Origin : egp
```

```
Attribute value : MED 0, pref-val 0
```

```
State : valid, external, best
```

```
IP precedence : N/A
```

```
QoS local ID : N/A
```

```
Traffic index : N/A
```

```
Route type : Software as a Service access path quality advertisement route
```

```
SiteID : 0x00ffffff
```

```
DeviceID : 1
```

```
SaaSName : abc
```

```
SystemIP : 2.2.2.2
```

Delay : 20 ms
 Jitter : 4 ms
 Loss : 50 %
 CQI : 80

Table 44 Command output

Field	Description
Total number of routes	Total number of BGP IPv4 tunnel-encap-ext routes.
Paths	Number of routes: available—Number of valid routes. best—Number of optimal routes.
BGP routing table information of [2][16777216][abc]/296	Detailed information about BGP IPv4 tunnel-encap-ext route [2][0x00ffffff][abc]/296.
From	IP address of the BGP peer that advertised the route.
Rely Nexthop	Next hop IP address after route recursion. If no next hop IP address is found, this field displays not resolved .
Original nexthop	Original next hop address of the route. If the route was obtained from a BGP update message, the original next hop address is the next hop IP address in the message.
OutLabel	Outgoing label of the route. This field is not supported by the BGP IPv4 tunnel-encap-ext address family in the current software version.
RxPathID	Add-Path ID value of the received route. This field is not supported by the BGP IPv4 tunnel-encap-ext address family in the current software version.
TxPathID	Add-Path ID value of the sent route. This field is not supported by the BGP IPv4 tunnel-encap-ext address family in the current software version.
AS-path	AS_PATH attribute of the route. This attribute records the ASs the route has passed and avoids routing loops.
Origin	Origin of the route: igp—Originated in the current AS. egp—Learned through EGP. incomplete—Unknown origin.
Attribute value	BGP attributes of the route: MED—MED value for the destination network. localpref—Local preference value. pref-val—Preferred value. pre—Protocol preference value.
State	Route state: valid—Valid route. internal—Internal route. external—External route. local—Local route. best—Optimal route.
IP precedence	IP precedence of the route, in the range of 0 to 7. If the IP precedence is invalid, this field displays N/A .
QoS local ID	QoS local ID of the route, in the range of 1 to 4095. If the QoS local

Field	Description
	ID is invalid, this field displays N/A .
Traffic index	Traffic index in the range of 1 to 64. If the traffic index is invalid, this field displays N/A .
SiteID	Site ID
DeviceID	Device ID
SaaSName	SaaS cloud service name.
SystemIP	Site system IP address.
Delay	Delay for the path used to access the SaaS cloud service, in milliseconds.
Jitter	Jitter for the path used to access the SaaS cloud service, in milliseconds.
Loss	Packet loss ratio for the path used to access the SaaS cloud service, in permillage.
CQI	Approximate Comprehensive Quality Indicator (CQI) value for the path used to access the SaaS cloud service.

Display advertisement information for BGP IPv4 tunnel-encap-ext route [1][10][10][100]/40.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext [1][10][10][100]/40 advertise-info
```

```
BGP local router ID: 1.1.1.1
```

```
Local AS number: 100
```

```
Total number of routes: 1
```

```
Paths: 1 best
```

```
BGP routing table information of [1][10][10][100]/40:
```

```
Advertised to peers (1 in total):
```

```
3.3.3.3
```

Table 45 Command output

Field	Description
Total number of routes	Total number of BGP IPv4 tunnel-encap-ext routes.
Paths	Number of optimal routes destined for the specified destination network.
BGP routing table information of [1][10][10][100]/40	Advertisement information about BGP IPv4 tunnel-encap-ext route [1][10][10][100]/40.
Advertised to peers (1 in total)	Peers to which the route has been advertised and total number of the peers.

Display statistics about BGP IPv4 tunnel-encap-ext routes advertised to peer 2.2.2.2.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext peer 2.2.2.2 advertised-routes statistics
```

```
Advertised routes total: 1
```

Display statistics about BGP IPv4 tunnel-encap-ext routes received from peer 2.2.2.2.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext peer 2.2.2.2 received-routes statistics
```

```
Received routes total: 1
```

Table 46 Command output

Field	Description
Advertised routes total	Total number of routes advertised to the peer.
Received routes total	Total number of routes received from the peer.

Display statistics about BGP IPv4 tunnel-encap-ext routes.

```
<Sysname> display bgp routing-table ipv4 tnl-encap-ext statistics
```

```
Total number of routes: 4
```

Table 47 Command output

Field	Description
Total number of routes	Total number of BGP IPv4 tunnel-encap-ext routes.

display sdwan peer-connection status

Use **display sdwan peer-connection status** to display SSL connection status on a CPE.

Syntax

```
display sdwan peer-connection status [ system-ip system-ip-address ] [ ipv4 | ipv6 ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

system-ip *system-ip-address*: Specifies an SDWAN server by its system IP address. If you do not specify an SDWAN server, this command displays status information for all SSL connections on the device.

ipv4: Displays status information for IPv4 SSL connections.

ipv6: Displays status information for IPv6 SSL connections.

Usage guidelines

If you do not specify the **ipv4** or **ipv6** keyword, this command displays status information for both IPv4 SSL connections and IPv6 SSL connections.

Examples

Display status information for all SSL connections on the device.

```
<Sysname> display sdwan peer-connection status
```

```
System IP      : 1.1.1.1
```

```
Peer IP/port: 10.0.0.1/7000
```

```
VPN instance: vpn1
```

Status : Connected

System IP : 1.1.1.1

Peer IP/port: 10::1/7000

VPN instance: vpn1

Status : Init

Table 48 Command output

Field	Description
System IP	System IP address of an SDWAN server.
Peer IP/port	IP address and listening TCP port number of the SDWAN server.
VPN instance	VPN instance of the SDWAN server.
Status	SSL connection state: • Init. • Connecting. • Connected. • Close.

Related commands

display sdwan server status

sdwan server

display sdwan server status

Use **display sdwan server status** to display SDWAN server status on an RR.

Syntax

display sdwan server status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display SDWAN server status on an RR.

```
<Sysname> display sdwan server status
```

SDWAN server: Enabled

SDWAN server listening port: 10030

Table 49 Command output

Field	Description
SDWAN server	SDWAN server state: • Enabled. • Disabled.
SDWAN server listening	TCP port number that the SDWAN server is listening to.

Field	Description
port	

Related commands

sdwan server enable

sdwan server port

display sdwan site-tte

Use **display sdwan site-tte** to display transport tunnel endpoint (TTE) information on an SDWAN device.

Syntax

display sdwan site-tte [**site-id** *site-id*] [**verbose**] [**ipv4** | **ipv6**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

site-id *site-id*: Specifies a site by its ID, in the range of 1 to 65535. If you do not specify a site, the command displays TTE information for all sites.

verbose: Displays detailed TTE information for sites. If you do not specify this keyword, the command displays brief TTE information for sites.

ipv4: Displays TTE information for IPv4 SDWAN tunnels.

ipv6: Displays TTE information for IPv6 SDWAN tunnels.

Usage guidelines

If you do not specify the **ipv4** or **ipv6** keyword, this command displays TTE information for both IPv4 SDWAN tunnels and IPv6 SDWAN tunnels.

Examples

Display brief TTE information for all sites.

```
<Sysname> display sdwan site-tte
```

```
Site ID: 20 (local)
```

```
Total number of TTEs: 1
```

```
*****
```

DevID	SysIP	IfID	Status	Encap	NAT	SA	RDID	TNID
20	1.1.1.9	20	UP	UDP IPv4	Disabled	Disabled	rda	tna

```
Site ID: 10
```

```
Total number of TTEs: 2
```

```
*****
```

DevID	SysIP	IfID	Status	Encap	NAT	SA	RDID	TNID
10	1.1.1.10	30	UP	UDP IPv4	Disabled	Disabled	rda	tna
10	1.1.1.10	40	UP	UDP IPv4	Disabled	Disabled	rda	tnb

Table 50 Command output

Field	Description
Site ID	Site ID. If (local) is displayed next to the site ID, the site is the local site.
Total number of TTEs	Total number of TTEs at the site.
DevID	Device ID.
SysIP	System IP address of the device.
IfID	SDWAN tunnel interface ID.
Status	TTE state: • UP. • DOWN.
Encap	SDWAN tunnel encapsulation method: • UDP IPv4—IPv4 tunnel in UDP encapsulation. • UDP IPv6—IPv6 tunnel in UDP encapsulation.
NAT	NAT state: • Enabled. • Disabled. • N/A—The state is unknown.
SA	SA state: • Enabled. • Disabled. • NA—The state is unknown.
RDID	Routing domain ID of the TTE.
TNID	Transport network ID of the TTE.

Display detailed TTE information for site 20.

```
<Sysname> display sdwan site-tte site-id 20 verbose
Site ID: 20 (local)
Site name: fenzhi
Site role: CPE
Device ID: 20
System IP: 1.1.1.9
Interface ID: 20
Group ID: 3
Interface name: Tunnel10
Status: UP
Encapsulation protocol: UDP IPv4
Encapsulation port: 3000
Tunnel destination VPN index: 0
Transport destination VPN index: 0
NAT: Disabled
NAT type: -
NAT public IP: -
NAT public port: -
SA: Disabled
Routing domain: rda (10)
```

Transport network: tna (10)
 Out physical interface: GigabitEthernet1/0/3
 Source IP: 172.1.1.1

Table 51 Command output

Field	Description
Site ID	Site ID. If (local) is displayed next to the site ID, the site is the local site.
Site role	Device role: • CPE. • RR—Route reflector. • NAT-transfer.
Interface ID	SDWAN tunnel interface ID.
Group ID	SDWAN tunnel group ID.
Interface name	SDWAN tunnel interface name.
Status	TTE state: • UP. • DOWN.
Encapsulation protocol	SDWAN tunnel encapsulation method: • UDP IPv4—IPv4 tunnel in UDP encapsulation. • UDP IPv6—IPv6 tunnel in UDP encapsulation.
Encapsulation port	Source UDP port number in SDWAN tunneled packets.
NAT	NAT state: • Enabled. • Disabled. • NA—The state is unknown.
NAT type	NAT type: • Full Cone NAT. • Restricted Cone NAT. • Port Restricted Cone NAT. • Symmetric NAT. • NO NAT. • Static NAT. The NAT type is unknown if this field displays a hyphen (-).
NAT public IP	Public IP address after NAT.
NAT public port	TCP port number after NAT.
SA	SA state: • Enabled. • Disabled. • NA—The state is unknown.
Routing domain	Routing domain name and ID of the TTE, in the format of <i>domain-name (domain-id)</i> .
Transport network	Transport network name and ID of the TTE, in the format of <i>network-name (network-id)</i> .
Out physical interface	Local physical output interface of the TTE.

Field	Description
Source IP	Source IP address of the SDWAN tunnel for the TTE.

Related commands

display sdwan tte connection

display sdwan tte connection

Use **display sdwan tte connection** to display TTE connection information on the device.

Syntax

display sdwan tte connection [**site-id** *site-id* | **system-ip** *system-ip-address*] [**reachable** | **unreachable**] [**ipv4** | **ipv6**] [**collaboration**]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

site-id *site-id*: Specifies a remote site by its ID, in the range of 1 to 65535. If you do not specify a remote site, this command displays TTE connection information for all sites.

system-ip *system-ip-address*: Specifies a remote device by its system IP address. If you do not specify a system IP address, this command displays TTE connection information for all system IP addresses.

reachable: Displays TTE connections reachable to system IP addresses.

unreachable: Displays TTE connections unreachable to system IP addresses.

ipv4: Displays TTE connections on IPv4 SDWAN tunnels.

ipv6: Displays TTE connections on IPv6 SDWAN tunnels.

collaboration: Displays TTE connections synchronized to the device through the RIR collaboration channel. If you do not specify this keyword, the command displays local TTE connections on the device.

Usage guidelines

If you do not specify the **reachable** or **unreachable** keyword, this command displays both TTE connections reachable to system IP addresses and TTE connections unreachable to system IP addresses.

If you do not specify the **ipv4** or **ipv6** keyword, this command displays TTE connections on both IPv4 SDWAN tunnels and IPv6 SDWAN tunnels.

Examples

Display information about all TTE connections on the device.

```
<Sysname> display sdwan tte connection
Destination SiteID/DevID/IfID/SysIP: 30/50/35/50.50.50.30
Destination IP/port: 200.200.200.30/3000
Source SiteID/DevID/IfID/SysIP: 20/55/30/50.50.50.10
Source IP/port: 200.200.200.10/3000
```

Destination SiteID/DevID/IfID/SysIP: 30/50/35/50.50.50.30
Destination IP/port: 200::30/3000
Source SiteID/DevID/IfID/SysIP: 50/10/20/50.50.50.10
Source IP/port: 200.200.200.10/300
Number of connections: 2

Table 52 Command output

Field	Description
Destination SiteID/DevID/IfID/SysIP	Site ID, device ID, tunnel interface ID, and system IP address of a peer device.
Destination IP/port	Destination IP address and TCP port number in SDWAN tunneled packets.
Source SiteID/DevID/IfID/SysIP	Site ID, device ID, tunnel interface ID, and system IP address of the local device.
Source IP/port	Source IP address and source TCP port number in SDWAN tunneled packets.
Number of connections	Number of TTE connections.

Related commands

display sdwan site-tte

reset sdwan tte connection

evpn-sdwan nexthop-recursive priority-color-only

Use **evpn-sdwan nexthop-recursive priority-color-only** to configure the device to perform next hop recursion based on only the Priority-Color attribute for SDWAN-encapsulated IP prefix advertisement routes.

Use **undo evpn-sdwan nexthop-recursive priority-color-only** to restore the default.

Syntax

evpn-sdwan nexthop-recursive priority-color-only

undo evpn-sdwan nexthop-recursive priority-color-only

Default

The device performs next hop recursion first based on the NEXT_HOP attribute and then the Priority-Color attribute for an IP prefix advertisement route that has the Priority-Color attribute after it receives that route.

Views

BGP EVPN address family view

Predefined user roles

network-admin

Usage guidelines

Application scenario

Use this command in an SDWAN scenario that uses the Priority-Color attribute for traffic rerouting or load balancing.

By default, the device performs next hop recursion for IP prefix advertisement routes based on both the NEXT_HOP and Priority-Color attributes after it receives these routes if these routes have the Priority-Color attribute. The recursion procedure is as follows for an IP prefix advertisement route:

- Typically, the address in the NEXT_HOP attribute is the system IP address of a remote CPE. The device looks up for a matching TTE connection based on the address. The SDWAN tunnel interface of the matching TTE connection is the next hop output interface obtained through next hop recursion for the IP prefix advertisement route.
- Each Priority-Color attribute includes the site ID information of a remote CPE or the site ID and device ID information of a remote CPE. The device looks up for matching TTE connections based on the information. The SDWAN tunnel interfaces of the matching TTE connections are the next hop output interfaces obtained through next hop recursion for the IP prefix advertisement route based on the Priority-Color attributes.

When the device receives packets that match an IP prefix advertisement route, it forwards the packets as follows:

- If BGP load balancing is not configured, the device forwards the packets over an SDWAN tunnel obtained through next hop recursion based on the NEXT_HOP attribute of the IP prefix advertisement route. When that SDWAN tunnel is not available, the device uses the SDWAN tunnel obtained through next hop recursion based on the Priority-Color attribute to forward the packets.
- If BGP load balancing is configured, the device can forward the packets over the following SDWAN tunnels for load balancing:
 - The SDWAN tunnel obtained through next hop recursion based on the NEXT_HOP attribute of the IP prefix advertisement route.
 - The SDWAN tunnels obtained through next hop recursion based on the Priority-Color attributes of the IP prefix advertisement route.

Based on the above mechanism, when the forwarding path obtained through next hop recursion based on the NEXT_HOP attribute is not available, the device still can forward VPN traffic along the forwarding path obtained through next hop recursion based on the Priority-Color attribute. The latter path is a backup for the former path. They provide rerouting and load balancing services for traffic.

The Priority-Color attribute is easy to configure, and the device can flexibly control the SDWAN forwarding path through this attribute. To perform next hop recursion for IP prefix advertisement routes that have the Priority-Color attribute based on only the Priority-Color attribute, use this command.

Working mechanism

With this command, when the device receives an IP prefix advertisement route that has the Priority-Color attribute, it does not perform next hop recursion based on the NEXT_HOP attribute. Instead, it performs next hop recursion directly based on the Priority-Color attribute. When the device receives packets that match the IP prefix advertisement route, it forwards the packets to an SDWAN tunnel obtained through next hop recursion based on only the Priority-Color attribute. In this way, the forwarding path is not restricted by the NEXT_HOP attribute of the IP prefix advertisement route. To adjust the forwarding path, you only need to modify the Priority-Color attribute.

Restrictions and guidelines

This command takes effect only on SDWAN-encapsulated IP prefix advertisement routes that have the Priority-Color attribute.

Examples

Configure the device to perform next hop recursion based on only the Priority-Color attribute for SDWAN-encapsulated IP prefix advertisement routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn evpn
```

```
[Sysname-bgp-default-ipv6] evpn-sdwan nexthop-recursive priority-color-only
```

evpn sdwan routing-enable

Use **evpn sdwan routing-enable** to enable EVPN to advertise SDWAN routes.

Use **undo evpn sdwan routing-enable** to disable EVPN from advertising SDWAN routes.

Syntax

evpn sdwan routing-enable

undo evpn sdwan routing-enable

Default

EVPN does not advertise SDWAN routes.

Views

VPN instance IPv4 address family view

VPN instance IPv6 address family view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to advertise VPN routes as BGP EVPN IP prefix advertisement routes in SDWAN encapsulation to peers. When the device receives BGP EVPN IP prefix advertisement routes in SDWAN encapsulation from the peers, it adds the routes to the routing table of the VPN instance.

Use this command in conjunction with the **peer advertise encap-type sdwan** command executed in BGP EVPN address family view.

Examples

In IPv4 address family view of VPN instance **vpna**, enable EVPN to advertise SDWAN routes.

```
<Sysname> system-view
```

```
[Sysname] ip vpn-instance vpna
```

```
[Sysname-vpn-instance-vpna] address-family ipv4
```

```
[Sysname-vpn-ipv4-vpna] evpn sdwan routing-enable
```

Related commands

peer advertise encap-type sdwan

reset sdwan tte connection

Use **reset sdwan tte connection** to clear SDWAN TTE connections.

Syntax

reset sdwan tte connection [**interface** *interface-type interface-number* [**site-id** *site-id* **device-id** *device-id* **interface-id** *interface-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an SDWAN tunnel interface by its type and number. If you do not specify an SDWAN tunnel interface, this command clears TTE connections for all SDWAN tunnel interfaces.

site-id *site-id* **device-id** *device-id* **interface-id** *interface-id*: Specifies an interface on a device at a site. The *site-id* argument represents the site ID, in the range of 1 to 65535. The *device-id* argument represents the device ID, in the range of 1 to 255. The *interface-id* argument represents the interface ID, in the range of 1 to 255. If you do not specify this option, the command clears all TTE connections for the specified SDWAN tunnel interface.

Usage guidelines

Clearing the TTE connections to a remote device also deletes the routes destined for the system IP address of that remote device. As a result, data packet forwarding is interrupted.

Clearing TTE connections between a CPE and an RR also interrupts the BGP sessions between them.

Examples

```
# Clear TTE connections for SDWAN tunnel interface Tunnel 1.
```

```
<Sysname> reset sdwan tte connection interface tunnel 1
```

Related commands

display sdwan tte connection

peer advertise encap-type sdwan

Use **peer advertise encap-type sdwan** to enable advertisement of EVPN routes in SDWAN encapsulation to a peer or peer group.

Use **undo peer advertise encap-type sdwan** to disable advertisement of EVPN routes in SDWAN encapsulation to a peer or peer group.

Syntax

peer { *group name* | *ipv4-address* [*mask-length*] } **advertise encap-type sdwan**

undo peer { *group name* | *ipv4-address* [*mask-length*] } **advertise encap-type sdwan**

Default

BGP does not advertise EVPN routes in SDWAN encapsulation to a peer or peer group.

Views

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must already exist.

ipv4-address: Specifies a peer by its IPv4 address. The peer must already exist.

mask-length: Specifies a mask length in the range of 0 to 32. To specify a subnet, you must specify both the *ipv4-address* and *mask-length* arguments.

Usage guidelines

Use this command on CPEs and RRs. On a CPE, use this command in conjunction with the **evpn sdwan routing-enable** command executed in VPN instance IPv4 address family view.

Examples

Configure BGP to advertise EVPN routes in SDWAN encapsulation to peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn evpn
[Sysname-bgp-default-evpn] peer 1.1.1.1 advertise encap-type sdwan
```

Related commands

evpn sdwan routing-enable

sdwan bfd enable

Use **sdwan bfd enable** to use BFD to test the connectivity of TTE connections on an SDWAN tunnel.

Use **undo sdwan bfd enable** to restore the default.

Syntax

sdwan bfd enable [**template** *template-name*]

undo sdwan bfd enable

Default

BFD is not used to test the connectivity of TTE connections on an SDWAN tunnel. The device uses keepalive packets to test the connectivity of TTE connections on an SDWAN tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

template *template-name*: Specifies a BFD template by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a BFD template or the specified BFD template does not exist, the device uses the default BFD session parameters.

Usage guidelines

With this command, the local device periodically sends BFD control packets to the remote device over all TTE connections on an SDWAN tunnel. If the device does not receive any BFD control packets from the remote device over a TTE connection within the detection period, it determines that the TTE connection is unreachable to the remote device. For more information about BFD, see *High Availability Configuration Guide*.

If BFD is used to test the connectivity of TTE connections on an SDWAN tunnel, you must use this command at both ends of the SDWAN tunnel.

If this command is used on an SDWAN tunnel interface, the device determines the connectivity of TTE connections on that SDWAN tunnel based on the BFD detection result. If this command is not used on an SDWAN tunnel interface, the device determines the connectivity of TTE connections on that SDWAN tunnel based on the keepalive result.

Examples

On SDWAN tunnel interface Tunnel 1, configure BFD to test the connectivity of TTE connections on the SDWAN tunnel.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] sdwan bfd enable template aa
```

Related commands

sdwan keepalive

sdwan device-id

Use **sdwan device-id** to assign an ID to the device.

Use **undo sdwan device-id** to restore the default.

Syntax

sdwan device-id *device-id*

undo sdwan device-id

Default

No ID is assigned to the device.

Views

System view

Predefined user roles

network-admin

Parameters

device-id: Specifies an ID for the device, in the range of 1 to 255.

Usage guidelines

The device ID uniquely identifies the device at a site.

Examples

Assign ID 2 to the device.

```
<Sysname> system-view
[Sysname] sdwan device-id 2
The current configuration will lead to offline. Are you sure? [Y/N]:
```

Related commands

display sdwan site-tte

sdwan encapsulation global-udp-port

Use **sdwan encapsulation global-udp-port** to specify a global source UDP port number for SDWAN tunneled packets.

Use **undo sdwan encapsulation global-udp-port** to restore the default.

Syntax

sdwan encapsulation global-udp-port *port-number*

undo sdwan encapsulation global-udp-port

Default

The global source UDP port number is 4799 for SDWAN tunneled packets.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a global source UDP port number for SDWAN tunneled packets, in the range of 1 to 65535. As a best practice, do not specify a known port number in the range of 1 to 1023.

Usage guidelines

All devices that belong to the same SDWAN routing domain must use the same source UDP port number.

You can specify a source UDP port number for SDWAN tunneled packets both in system view and in tunnel interface view.

- The source UDP port number specified in system view applies to all SDWAN tunnel interfaces.
- The source UDP port number specified in tunnel interface view applies only to one tunnel interface.

For a tunnel interface, the source UDP port number specified in tunnel interface view takes precedence over that specified in system view. If no source UDP port number is specified in tunnel interface view, the source UDP port number specified in system view applies.

Examples

Specify port number 5000 as the global source UDP port number for SDWAN tunneled packets.

```
<Sysname> system-view
```

```
[Sysname] sdwan encapsulation global-udp-port 5000
```

sdwan encapsulation udp-port

Use **sdwan encapsulation udp-port** to specify a source UDP port number for SDWAN tunneled packets in UDP encapsulation mode.

Use **undo sdwan encapsulation udp-port** to restore the default.

Syntax

sdwan encapsulation udp-port *port-number* [**dynamic** [*time*]]

undo sdwan encapsulation udp-port

Default

The source UDP port number for SDWAN tunneled packets is the global source UDP port number for SDWAN tunneled packets.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

port-number: Specifies a source UDP port number in the range of 1 to 65535. As a best practice, do not specify a known port number in the range of 1 to 1023.

dynamic: Obtains UDP port numbers dynamically.

time: Specifies the delay time for switching the dynamic UDP port number. The value range is 30 to 1800, in seconds. The default value is 180.

Usage guidelines

If the **dynamic** keyword is specified, the device requests a UDP port number from the UDP protocol stack when the UDP port number specified by this command is unavailable.

You can specify a source UDP port number for SDWAN tunneled packets both in system view and in tunnel interface view.

- The source UDP port number specified in system view applies to all SDWAN tunnel interfaces.
- The source UDP port number specified in tunnel interface view applies only to one tunnel interface.

For a tunnel interface, the source UDP port number specified in tunnel interface view takes precedence over that specified in system view. If no source UDP port number is specified in tunnel interface view, the source UDP port number specified in system view applies.

In a full-mesh scenario, do not specify the **dynamic** keyword as a best practice. The dynamic mode might trigger TTE reconnections of the device with other branches, causing traffic interruption or flapping issues.

Examples

Specify 5000 as the source UDP port number of SDWAN tunneled packets.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] sdwan encapsulation udp-port 5000
```

Related commands

display sdwan site-tte

sdwan group-id

Use **sdwan group-id** to specify a group ID for an SDWAN tunnel.

Use **undo sdwan group-id** to restore the default.

Syntax

sdwan group-id *group-id*

undo sdwan group-id

Default

No group ID is specified for an SDWAN tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a group ID in the range of 1 to 65535.

Usage guidelines

Use this command to control the establishment of TTE connections in a more fine and flexible manner. In the same routing domain, only tunnel interfaces that have the same group ID and belong to the same transport network can establish TTE connections.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify group ID 22 for SDWAN tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] sdwan group-id 22
The current configuration will lead to TTE offline. Continue anyway? [Y/N]:
```

sdwan interface-id

Use **sdwan interface-id** to assign an interface ID to an SDWAN tunnel interface.

Use **undo sdwan interface-id** to restore the default.

Syntax

sdwan interface-id *interface-id*

undo sdwan interface-id

Default

No interface ID is assigned to an SDWAN tunnel interface.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

interface-id: Specifies an interface ID for the SDWAN tunnel interface, in the range of 1 to 255.

Usage guidelines

The device supports multiple SDWAN tunnel interfaces. An interface ID uniquely identifies an SDWAN tunnel interface on the device.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Assign interface ID 10 to SDWAN tunnel interface Tunnel 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] sdwan interface-id 10
The input configuration will be written to the device, changes may cause device offline.
Are you sure? [Y/N]:
```

Related commands

display sdwan site-tte

sdwan keepalive

Use **sdwan keepalive** to configure SDWAN keepalive settings.

Use **undo sdwan keepalive** to restore the default.

Syntax

sdwan keepalive interval *interval* [**retry** *retries*]

undo sdwan keepalive

Default

The keepalive interval is 10 seconds and the number of keepalive retries is 3 for an SDWAN tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval between sending keepalive requests, in the range of 1 to 32767 seconds.

retry *retries*: Specifies the number of times that the device continues to send keepalive packets without response before the TTE connection state is changed to unreachable. The value range for the *retries* argument is 1 to 255 and the default value is 3.

Usage guidelines

After an SDWAN tunnel is established, the local device sends keepalive requests to the remote device over all the TTE connections on the tunnel interface at the specified keepalive interval.

- If the local device receives a keepalive response from the remote device within a keepalive interval, it determines that a TTE connection is reachable to the remote device.
- If the local device cannot receive a keepalive response from the remote device on a TTE connection within a keepalive interval, it resends a keepalive request. If the local device still cannot receive a response within the keepalive interval multiplied by keepalive retries, it determines that the TTE connection is unreachable to the remote device. The device no longer forwards packets through the TTE connection.

In an RIR-SDWAN network, set the keepalive interval within the range of 1 to 5 seconds as a best practice.

If the **sdwan bfd enable** command is used on an SDWAN tunnel interface, the device determines the connectivity of TTE connections on that SDWAN tunnel based on the BFD detection result. If this command is not used on an SDWAN tunnel interface, the device determines the connectivity of TTE connections on that SDWAN tunnel based on the keepalive result.

Examples

On SDWAN tunnel interface 1, set the keepalive interval to 30 seconds and the number of keepalive retries to 5.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] sdwan keepalive interval 30 retry 5
```

Related commands

sdwan bfd enable

sdwan nat-global-ip

Use **sdwan nat-global-ip** to specify the post-NAT public IP address and port number for the source IP address and port number of tunneled packets.

Use **undo sdwan nat-global-ip** to restore the default.

Syntax

sdwan nat-global-ip *global-address* **global-port** *global-port*
undo sdwan nat-global-ip

Default

The post-NAT public IP address and port number are not specified for the source IP address and port number of tunneled packets.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

global-address: Specifies the post-NAT public IP address.

global-port: Specifies the post-NAT public port number, in the range of 1 to 65535.

Usage guidelines

Use this command on a CPE or RR if the CPE or RR is behind a NAT device and the NAT device is configured with static NAT. With this command, you do not need to configure STUN to detect the post-NAT public IP address and port number for the source IP address and port number of tunneled packets on the CPE or RR.

Using this command on a tunnel interface causes the device to disconnect all existing TTE connections established to the tunnel interface. The device will reestablish these TTE connections based on the specified post-NAT public IP address and port number.

As a best practice, do not use this command if the public network cannot actively access the internal network.

Examples

Specify 10.1.1.1 and 5000 as the post-NAT public IP address and port number for the source IP address and port number of tunneled packets.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] sdwan nat-global-ip 10.1.1.1 global-port 5000
The current configuration will lead to TTE offline. Continue anyway? [Y/N]:
```

sdwan routing-domain

Use **sdwan routing-domain** to specify a routing domain for an SDWAN tunnel.

Use **undo sdwan routing-domain** to restore the default.

Syntax

sdwan routing-domain *domain-name* **id** *domain-id*
undo sdwan routing-domain

Default

No routing domain is specified for an SDWAN tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a routing domain by its name, a case-sensitive string of 1 to 31 characters. The string can contain only letters, digits, and dots (.).

domain-id: Specifies the ID of the routing domain, in the range of 1 to 65535.

Usage guidelines

Only CPEs and RRs that belong to the same routing domain can establish SDWAN tunnels with each other.

Examples

Specify the routing domain named **abc** and with ID 2000 for SDWAN tunnel 1.

```
<Sysname> system-view
```

```
[Sysname] interface tunnel 1 mode sdwan udp
```

```
[Sysname-Tunnel1] sdwan routing-domain abc id 2000
```

Related commands

display sdwan site-tte

sdwan server

Use **sdwan server** to specify an SDWAN server on a CPE.

Use **undo sdwan server** to remove an SDWAN server from a CPE.

Syntax

sdwan server system-ip *system-ip-address* { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo sdwan server system-ip *system-ip-address* { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

Default

No SDWAN servers are specified on a CPE.

Views

System view

Predefined user roles

network-admin

Parameters

system-ip *system-ip-address*: Specifies an SDWAN server by its system IP.

ip *ipv4-address*: Specifies the IPv4 address of the SDWAN server. The IPv4 address must be reachable and must be on the RR where SDWAN server is enabled.

ipv6 *ipv6-address*: Specifies the IPv6 address of the SDWAN server. The IPv6 address must be reachable and must be on the RR where SDWAN server is enabled.

port *port-number*: Specifies a TCP port number used to establish connections with the SDWAN server. Make sure the port number is the same as the TCP listening port number configured for the SDWAN server on the RR. The value range for the *port-number* argument is 1 to 65535, and the default value is 2004.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the SDWAN server belongs. The *vpn-instance-name* argument represents the VPN instance name, which is a case-sensitive string of 1 to 31 characters. If the SDWAN server belongs to the public network, do not specify this option.

Usage guidelines

With this command, a CPE can act as an SDWAN client to establish an SSL connection with the specified SDWAN server (RR).

Repeat this command to specify multiple SDWAN servers on a CPE.

Examples

On a CPE, specify the SDWAN server at 10.1.1.1 and with system IP address 192.168.0.1.

```
<Sysname> system-view
[Sysname] sdwan server system-ip 192.168.0.1 ip 10.1.1.1
```

Related commands

display sdwan peer-connection status

sdwan server enable

Use **sdwan server enable** to enable SDWAN server on an RR.

Use **undo sdwan server enable** to disable SDWAN server on an RR.

Syntax

sdwan server enable

undo sdwan server enable

Default

SDWAN server is disabled on an RR.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command only on an RR. With this command, the RR can listen to the CPEs for SSL connection requests and establish SSL connections with the CPEs. After SSL connection establishment, the CPEs advertise their local TTE and IPsec SA information to the RR and the RR advertises its local TTE and IPsec SA information to the CPEs. Then, the RR and CPEs can finish SDWAN tunnel establishment.

When you enable SDWAN server on an RR and the RR does not have a digital certificate, digital certificate request is triggered. It takes some time to request a digital certificate. For more information about digital certificates, see PKI configuration in *Security Configuration Guide*.

Examples

Enable SDWAN server on an RR.

```
<Sysname> system-view
[Sysname] sdwan server enable
Please wait.....Done.
```

Related commands

display sdwan server status

sdwan ssl-server-policy

sdwan server port

Use **sdwan server port** to specify the TCP port that the SDWAN server listens to on an RR.

Use **undo sdwan server port** to restore the default.

Syntax

sdwan server port *port-number*

undo sdwan server port

Default

The SDWAN server on an RR listens to TCP port 2004.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

This command is not supported in FIPS mode.

If SDWAN server has been enabled before you change the TCP port number, the system automatically restarts the SDWAN server after you change the TCP port number. Connections that have been established between CPEs and the SDWAN server are not lost. Connections being established between CPEs and the SDWAN server are lost. To reestablish the connections, you must specify the same TCP port number as the SDWAN server on the CPEs.

Examples

```
# Specify 3500 as the TCP listening port number of the SDWAN server on an RR.
```

```
<Sysname> system-view
```

```
[Sysname] sdwan server port 3500
```

Related commands

display sdwan server status

sdwan server enable

sdwan site-id

Use **sdwan site-id** to specify a site ID for the device.

Use **undo sdwan site-id** to restore the default.

Syntax

sdwan site-id *site-id*

undo sdwan site-id

Default

No site ID is specified for the device.

Views

System view

Predefined user roles

network-admin

Parameters

site-id: Specifies a site ID for the device, in the range of 1 to 65535.

Usage guidelines

A site ID uniquely identifies a customer site in an SDWAN network.

Examples

```
# Specify site ID 2 for the device.
```

```
<Sysname> system-view
```

```
[Sysname] sdwan site-id 2
```

```
The current configuration will lead to offline. Are you sure? [Y/N]:
```

Related commands

display sdwan site-tte

sdwan site-name

Use **sdwan site-name** to specify the name of the site to which the device belongs.

Use **undo sdwan site-name** to restore the default.

Syntax

sdwan site-name *site-name*

undo sdwan site-name

Default

No site name is specified for the device.

Views

System view

Predefined user roles

network-admin

Parameters

site-name: Specifies a site name for the device, a case-sensitive string of 1 to 255 characters.

Usage guidelines

A site name can describe the site location and functions, which facilitates users to identify the site in an SDWAN network. A site name does not uniquely identify a site. You can specify the same site name for multiple devices.

Examples

```
# Specify site name fenbu for the device.
```

```
<Sysname> system-view
```

```
[Sysname] sdwan site-name fenbu
```

Related commands

display sdwan site-tte

sdwan site-role

Use **sdwan site-role** to specify a site role for the device.

Use **undo sdwan role** to restore the default.

Syntax

sdwan site-role { cpe | nat-transfer | rr } *

undo sdwan site-role

Default

No site role is specified for the device.

Views

System view

Predefined user roles

network-admin

Parameters

cpe: Specifies the CPE role.

nat-transfer: Specifies the NAT transfer role.

rr: Specifies the route reflector (RR) role.

Usage guidelines



IMPORTANT:

A site role change will cause SDWAN tunnel flapping and interrupt ongoing services. As a best practice, plan role configuration before you deploy the SDWAN network.

SDWAN supports the following site roles:

- **CPE**—Customer-side SDWAN tunnel endpoints.
- **RR**—Used to reflect TTE information and private routes among CPEs.
- **NAT transfer**—Used to establish forwarding paths for CPEs that must pass through NAT devices over the public network for intercommunication.

You must specify the same site role for all SDWAN devices at the same site.

Examples

Specify site role **CPE** for the device.

```
<Sysname> system-view
```

```
[Sysname] sdwan site-role cpe
```

The configuration will be written to the device, changes may cause device offline. Are you sure? [Y/N]:

Related commands

display sdwan site-tte

sdwan ssl-server-policy

Use **sdwan ssl-server-policy** to specify an SSL server policy on an RR for the RR to establish SSL connections with CPEs (SDWAN clients).

Use **undo sdwan ssl-server-policy** to restore the default.

Syntax

sdwan ssl-server-policy *policy-name*

undo sdwan ssl-server-policy

Default

No SSL server policy is specified on an RR for the RR to establish SSL connections with CPEs (SDWAN clients).

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

With this command, an RR uses the specified policy to establish SSL connections with CPEs. After SSL connection establishment, the CPEs advertise their local TTE and IPsec SA information to the RR and the RR advertises its local TTE and IPsec SA information to the CPEs. Then, the RR and the CPEs can finish SDWAN tunnel establishment.

Only one SSL server policy can be applied to an SSL connection. If you execute this command multiple times, the most recent configuration cannot take effect automatically. For the most recent configuration to take effect, you must execute the **undo sdwan server enable** command and then the **sdwan server enable** command to re-enable the SDWAN server.

For more information about SSL server policies, see SSL configuration in *Security Configuration Guide*.

If you do not specify an SSL server policy on an RR, the RR uses the self-signed certificate and the default settings of the SSL parameters to establish SSL connections with CPEs or the NAT transfer. The configuration is simple, but less secure.

Examples

On an RR, specify SSL server policy **CA_CERT** for the RR to establish SSL connections with CPEs (SDWAN clients).

```
<Sysname> system-view
```

```
[Sysname] sdwan ssl-server-policy CA_CERT
```

Related commands

display sdwan server status

sdwan server enable

sdwan server port

sdwan ssl-client-policy

Use **sdwan ssl-client-policy** to specify an SSL client policy on a CPE for the CPE to establish SSL connections with RRs (SDWAN servers).

Use **undo sdwan ssl-client-policy** to restore the default.

Syntax

sdwan ssl-client-policy *policy-name*

undo sdwan ssl-client-policy

Default

No SSL client policy is specified on a CPE for the CPE to establish SSL connections with RRs (SDWAN servers).

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

Only one SSL client policy can be applied to an SSL connection. If you execute this command multiple times, the most recent configuration takes effect. Modification to this command does not affect existing SDWAN SSL connections. It takes effect only on the SDWAN SSL connections established after the modification.

For more information about SSL client policies, see SSL configuration in *Security Configuration Guide*.

Examples

On a CPE, specify SSL client policy **abc** for the CPE to establish SSL connections with RRs (SDWAN servers).

```
<Sysname> system-view
```

```
[Sysname] sdwan ssl-client-policy abc
```

sdwan system-ip

Use **sdwan system-ip** to specify a system IPv4 address for the device.

Use **undo sdwan system-ip** to restore the default.

Syntax

sdwan system-ip *interface-type interface-number*

undo sdwan system-ip

Default

No system IPv4 address is specified for the device.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number. The primary IPv4 address of the specified interface is used as the system IPv4 address of the device.

Usage guidelines

The device uses the system IPv4 address to set up BGP sessions with other devices. In an RIR scenario, the system IPv4 address is also used as the inner destination IPv4 address of probe packets sent by the NQA client in NQA link connectivity probes. For more information about RIR, see *Layer 3—IP Routing Configuration Guide*.

For this command to take effect, you must specify a loopback interface that has an IPv4 address.

Examples

```
# Specify the primary IPv4 address of Loopback 0 as the system IPv4 address of the device.
```

```
<Sysname> system-view
```

```
[Sysname] sdwan system-ip loopback 0
```

Related commands

display sdwan site-tte

sdwan transport-network

Use **sdwan transport-network** to specify a transport network for an SDWAN tunnel.

Use **undo sdwan transport-network** to restore the default.

Syntax

sdwan transport-network *network-name* **id** *network-id* [**restrict**]

undo sdwan transport-network

Default

No transport network is specified for an SDWAN tunnel.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

network-name: Specifies a transport network by its name, a case-sensitive string of 1 to 31 characters. The string can contain only letters, digits, and dots (.).

network-id: Specifies the ID of the transport network, in the range of 1 to 65535.

restrict: Allows only tunnel interfaces that are specified the same routing domain and the same transport network ID to set up TTE connections. If you do not specify this keyword, the system allows tunnel interfaces that are specified the same routing domain to set up TTE connections regardless of whether their transport network IDs are the same.

Usage guidelines

An SDWAN tunnel interface is connected to a transport network. The transport network is uniquely identified by its name or ID.

Examples

```
# Specify a transport network named abc with ID 2000 for an SDWAN tunnel.
```

```
<Sysname> system-view
```

```
[Sysname] interface tunnel 1 mode sdwan udp
```

```
[Sysname-Tunnel1] sdwan transport-network abc id 2000
```

Related commands

display sdwan site-tte

sdwan vn-id

Use **sdwan vn-id** to specify a VN ID for a VPN instance.

Use **undo sdwan vn-id** to restore the default.

Syntax

sdwan vn-id *vn-id*

undo sdwan vn-id

Default

The VN ID is 0 for a VPN instance.

Views

VPN instance view.

Predefined user roles

network-admin

Usage guidelines

Packets from different tenants can be forwarded through the same SDWAN tunnel. To isolate the tenants, assign them to different VPN instances. Their packets will be distinguished according to the VN IDs of the VPN instances.

You can specify only one VN ID for a VPN instance in the current software version.

Examples

```
# Specify VN ID 123 for VPN instance vpna.
<Sysname> system-view
[Sysname] ip vpn-instance vpna
[Sysname-vpn-instance-vpna] sdwan vn-id 123
```

Related commands

evpn sdwan routing-enable

New feature: STUN

About STUN

Session Traversal Utilities for NAT (STUN) is a protocol that serves as a tool for other protocols in dealing with NAT traversal. STUN can determine the existence of a NAT device in the network and determine the IP address and port allocated by the NAT device to an endpoint. STUN runs over UDP and uses port 3478 by default.

Basic concepts

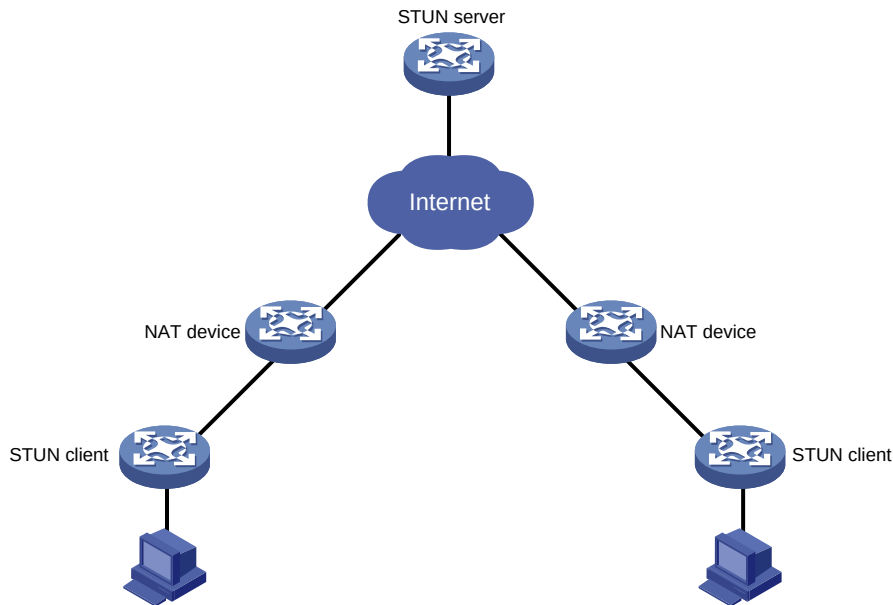
As shown in [Figure 21](#), STUN uses a client-server model that consists of a STUN client and a STUN server.

- **STUN client**—An entity that sends STUN requests and receives STUN responses.

- **STUN server**—An entity that receives STUN requests and sends STUN responses. A STUN server typically resides on the public network.

The STUN server and STUN client exchange STUN packets (Binding requests and Binding responses) to detect the IP address and port number assigned by a NAT device and the NAT type.

Figure 21 STUN network diagram



NAT mapping and filtering

In STUN, NAT mapping and NAT filtering are used to determine the type of NAT and therefore determine whether STUN works correctly. The related concepts are described as follows:

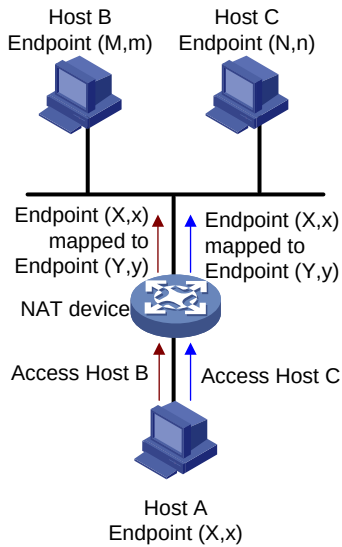
- **Endpoint**—A combination of an IP address and a port number. For example, Endpoint (X:x) indicates that the IP address and port number are X and x, respectively.
- **NAT mapping**—Maps an internal IP address and port number to an external IP address and port number for packets from the internal network to the external network. When an internal endpoint opens an outgoing session through a NAT device, the NAT device establishes a mapping between the internal IP address and port number and an external IP address and port number. Then, the NAT device forwards the packet based on the mapping.
- **NAT filtering**—Filters out packets from the external network to the internal network. To protect the internal network from attacks, the NAT device will discard attack packets and forward normal packets.

NAT mapping types

The following NAT mapping types are supported:

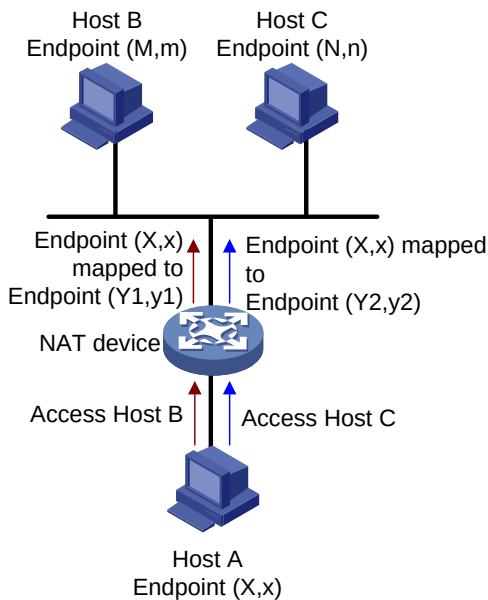
- **Endpoint-independent mapping (EIM)**—The NAT device uses the same mapping for all packets sent from the same internal IP address and port number to any external IP address and port number. As shown in [Figure 22](#), Endpoint (X:x) in the internal network is always mapped to Endpoint (Y:y) in the external network.

Figure 22 EIM



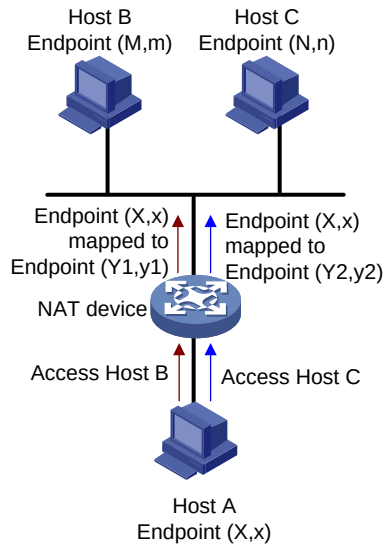
- **Address-dependent mapping (ADM)**—The NAT device uses the same mapping for all packets sent from the same internal IP address and port number to the same external IP address, regardless of the external port number. As shown in Figure 23, Endpoint (X:x) in the internal network is mapped to Endpoint (Y1:y1) in the external network when it accesses Host B. Endpoint (X:x) in the internal network is mapped to Endpoint (Y2:y2) in the external network when it accesses Host C. Y1:y1 equals Y2:y2 as long as M equals N.

Figure 23 ADM



- **Address and port-dependent mapping (APDM)**—The NAT device uses the same mapping for all packets sent from the same internal IP address and port number to the same external IP address and port number. As shown in Figure 24, Endpoint (X:x) in the internal network is mapped to Endpoint (Y1:y1) in the external network when it accesses Host B. Endpoint (X:x) in the internal network is mapped to Endpoint (Y2:y2) in the external network when it accesses Host C. Y1:y1 equals Y2:y2 if M equals N and m equals n.

Figure 24 APDM

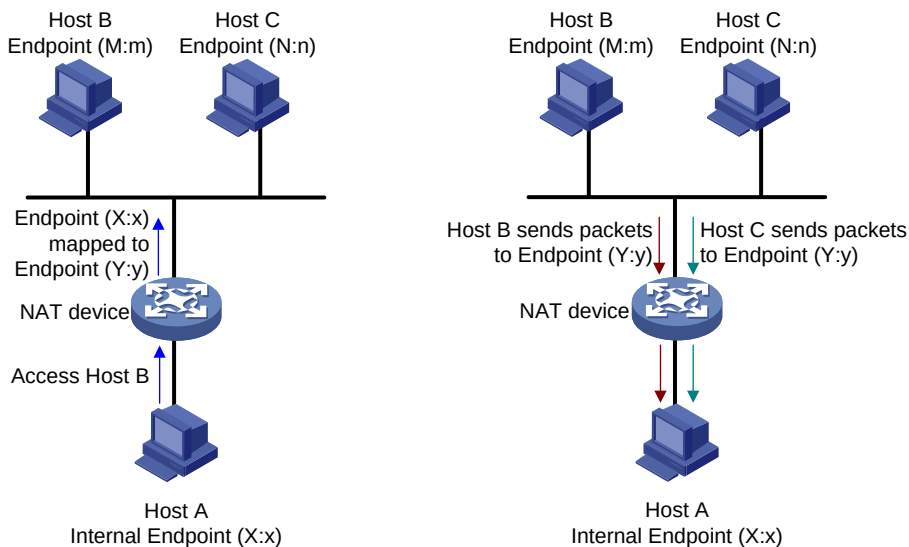


NAT filtering methods

The following NAT filtering types are supported:

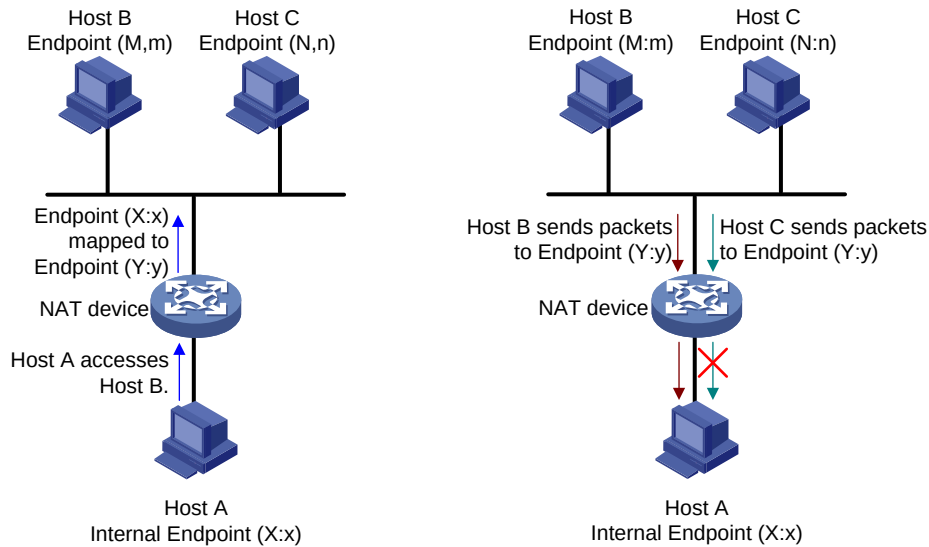
- **Endpoint-independent filtering (EIF)**—As shown in Figure 25, the NAT device filters out only packets not destined to the internal IP address and port number (Endpoint (X:x), regardless of the external IP address and port source. The NAT device forwards any packets destined to X:x.

Figure 25 EIF



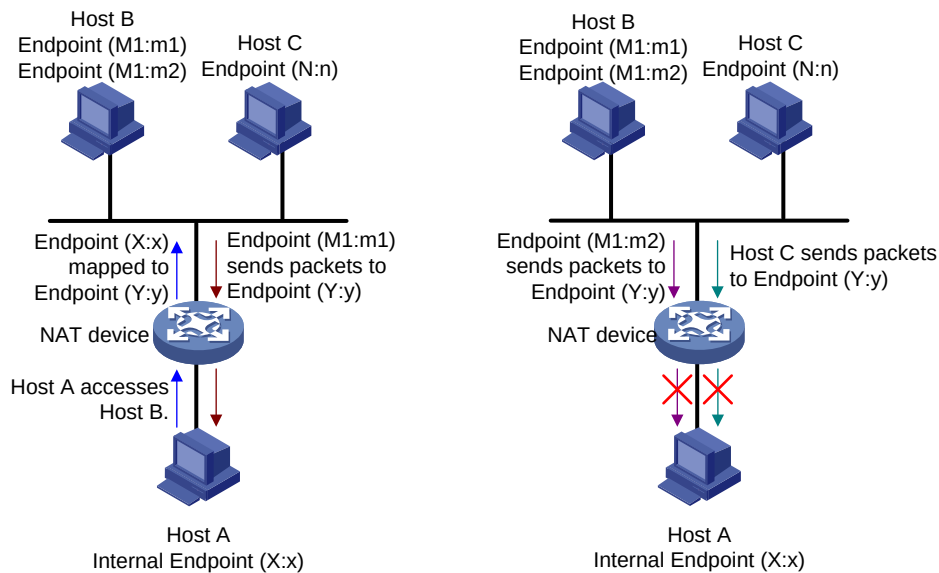
- **Address-dependent filtering (ADF)**—As shown in Figure 26, the NAT device filters out packets not destined to the internal address X:x. Additionally, the NAT device will filter out packets from Y:y destined for the internal endpoint X:x if X:x has not sent packets to Y: any port previously (independently of the port used by Y).

Figure 26 ADF



- **Address and port-dependent filtering (APDF)**—As shown in Figure 27, the NAT device filters out packets not destined to the internal address X:x. Additionally, the NAT device will filter out packets from Y:y destined for the internal endpoint X:x if X:x has not sent packets to Y:y previously.

Figure 27 APDF



NAT types

A NAT type is a combination of a NAT mapping type and a NAT filtering method. The following NAT types are supported:

- **Full cone NAT (EIM+EIF)**—Maps all requests from the same internal IP address and port number (IP1:Port1) to the same external IP address and port number (IP:Port). Additionally, any external host can send a packet to the internal host by sending a packet to the mapped external address.
- **Restricted cone NAT (EIM+ADF)**—Maps all requests from the same internal IP address and port number (IP1:Port1) to the same external IP address and port number (IP:Port). Unlike a full cone NAT, an external

host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

- **Port restricted cone NAT (EIM+APDF)**—Maps all requests from the same internal IP address and port number (IP1:Port1) to the same external IP address and port number (IP:Port). Unlike a restricted cone NAT, an external host (with IP address and port number IP2:Port2) can send a packet to the internal host only if the internal host had previously sent a packet to IP address and port number IP2:Port2.
- **Symmetric NAT (APDM+APDF)**—Maps all requests from the same internal IP address and port number (IP1:Port1), to a specific destination IP address and port number, to the same external IP address and port number. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Additionally, only the external host that receives a packet can send a UDP packet back to the internal host.

Application scenarios

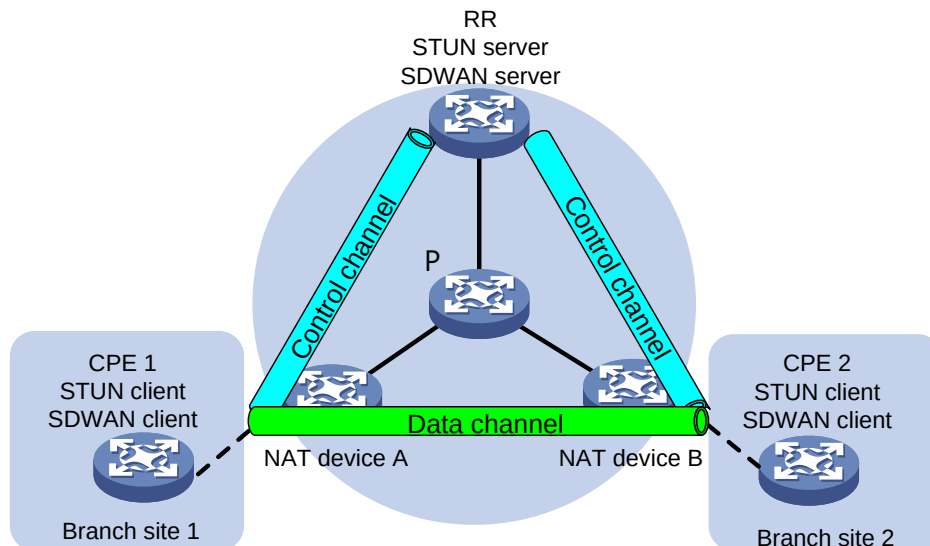
As shown in Figure 28, users at branch sites use private IP addresses so as to conserve IP address resources. After NAT devices translate the private IP addresses to public IP addresses, users at one branch site can access the headquarters.

IP addresses of the packets sent by a CPE will change after the packets pass through a NAT device. If the CPE cannot obtain its public IP address translated after NAT, it cannot establish a data channel with the other CPE. To resolve this issue, configure Session Traversal Utilities for NAT (STUN) in the SDWAN network. Typically, use CPEs as STUN clients and use the RR as the STUN server. The clients exchange packets with the server to identify whether NAT devices exist in the SDWAN network. If NAT devices exist, the clients obtain their public IP addresses and port numbers translated after NAT.

After a CPE (STUN client) obtains its public IP address and port number translated after NAT, it uses this public IP address to establish a data channel with the other CPE.

For more information about SDWAN tunnel establishment with NAT traversal, see *SDWAN Configuration Guide*.

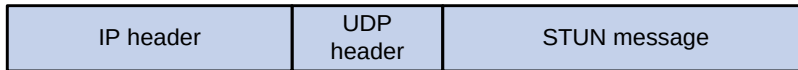
Figure 28 SDWAN tunnel establishment with NAT traversal



STUN packet structure

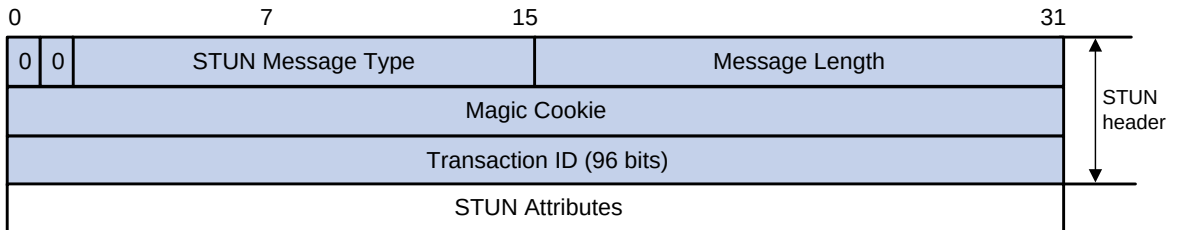
STUN uses UDP as the transport protocol. Figure 29 shows the format of a STUN packet.

Figure 29 STUN packet structure



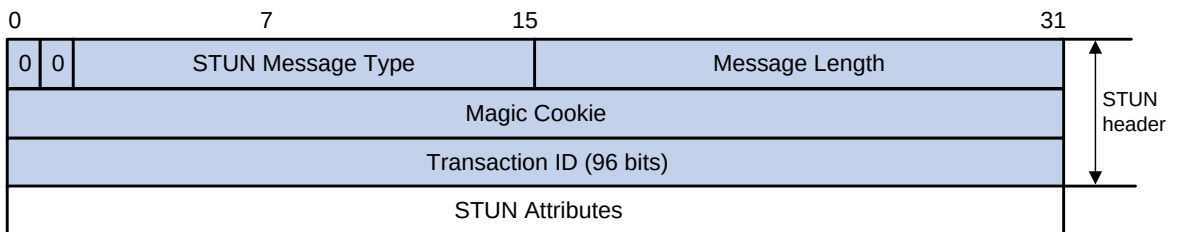
As shown in [Figure 30](#), a STUN message starts with a 20-byte STUN header followed by zero or more STUN attributes.

Figure 30 STUN message structure



As shown in [Figure 31](#), a STUN message starts with a 20-byte STUN header followed by zero or more STUN attributes.

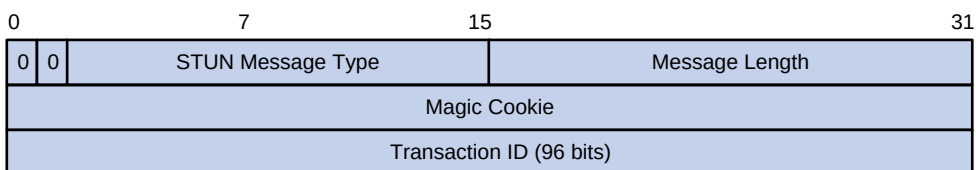
Figure 31 STUN message structure



STUN header

[Figure 32](#) shows the STUN header structure.

Figure 32 STUN header structure



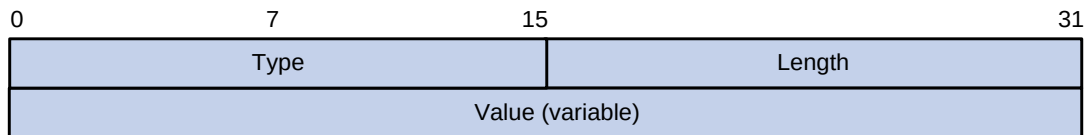
A STUN header contains the following fields:

- **STUN Message Type**—14-bit long and can only be Binding request or Binding response.
- **Message Length**—16-bit long. The message length does not include the STUN header.
- **Magic Cookie**—Contains the fixed value 0x2112A442. This field allows a server to detect if the client will understand certain attributes. In addition, it aids in distinguishing STUN packets from packets of other protocols when STUN is multiplexed with those other protocols on the same port.
- **Transaction ID**—Used to uniquely identify STUN transactions. The transaction ID is chosen by the STUN client for the request and echoed by the server in the response.

STUN attribute

Each STUN attribute is TLV (Type-Length-Value) encoded, with a 16-bit type, 16-bit length, and value.

Figure 33 Format of STUN attributes



The following are common STUN attributes:

- **CHANGE-REQUEST**—Carried in Binding requests. This attribute is used by the STUN client to request that the STUN server use a different address or port number when sending the response.
- **MAPPED-ADDRESS**—Carried in Binding responses. This attribute indicates the mapped IP address and port number of the client.
- **XOR-MAPPED-ADDRESS**—Carried in Binding responses. This field is identical to the MAPPED-ADDRESS attribute, except that the reflexive transport address is obfuscated through the XOR function.
- **RESPONSE-ORIGIN**—Carried in Binding responses. This attribute indicates the IP address and port number of the STUN server.
- **OTHER-ADDRESS**—Carried in Binding responses. This attribute indicates the alternate IP address and port number of the STUN server. Suppose the IP address and port number of the STUN server is Y1:YP1, and the alternate IP address and port number of the STUN server is Y2:YP2. Da represents the destination IP address in Binding requests sent by the STUN client, Dp represents the destination port number in Binding requests sent by the STUN client. If Da is Y1, the IP address in the OTHER-ADDRESS attribute is Y2. If Da is Y2, the IP address in the OTHER-ADDRESS attribute is Y1. If Dp is YP1, the port number in the OTHER-ADDRESS attribute is YP2. If Dp is YP2, the port number in the OTHER-ADDRESS attribute is YP1.

When the STUN client requests that the server use a different address or port number when sending the response:

- **Using a different address**—If the destination IP address of the Binding request is Y1, the alternate IP address is Y2, and vice versa. The STUN server uses the alternate IP address to send a response.
- **Using a different port number**—If the destination port number of the Binding request is YP1, the alternate port number is YP2, and vice versa. The STUN server uses the alternate port number to send a response.

If no alternate IP address is specified for a STUN server, the STUN server does not carry the **OTHER-ADDRESS** attribute in Binding responses. In this case, the STUN client cannot determine the NAT type.

How STUN works

The STUN client and STUN server exchange STUN packets to detect the NAT mapping type and NAT filtering method, therefore determining the NAT type.

NAT mapping type detection

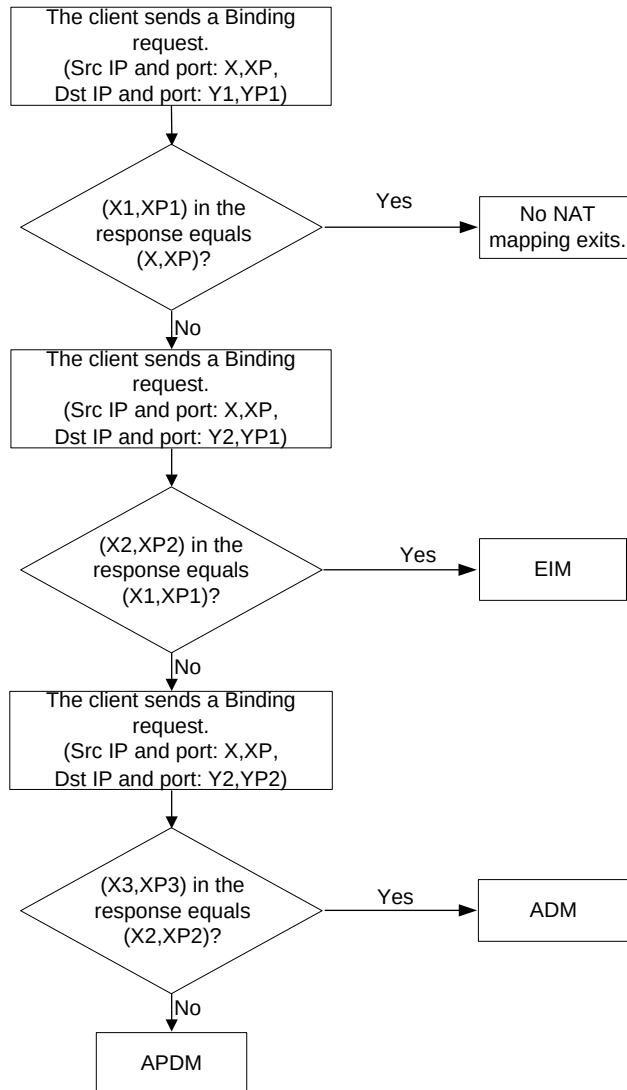
Suppose the IP address and port number of the STUN server is Y1:YP1, and the alternate IP address and port number of the STUN server is Y2:YP2. The IP address and port number of the STUN client is X:XP.

Figure 34 shows the process of NAT mapping type detection.

1. The STUN client sends a Binding request with source IP address and port number Endpoint (X:XP) to Endpoint (Y1:YP1) of the STUN server. The STUN server uses Endpoint (Y1:YP1) to send a Binding response to the STUN client. The Binding response includes the mapped Endpoint (X1:XP1) and another Endpoint (Y2:YP2) of the STUN server.

2. After receiving the Binding response, the STUN client checks whether Endpoint (X1:XP1) equals Endpoint (X:XP).
 - If yes, the client considers that no mapping exists.
 - If not, the client detects the mapping type as described in step 3.
3. The STUN client uses Endpoint (X:XP) to send a Binding request to Endpoint (Y2,YP1) of the STUN server. The STUN server uses Endpoint (Y2,YP1) to send a Binding response to the STUN client. The Binding response includes the mapped Endpoint (X2:XP2) of the STUN client.
4. After receiving the Binding response, the STUN client checks whether Endpoint (X2:XP2) equals Endpoint (X1:XP1) in step 1.
 - If yes, the client considers that the mapping type is EIM.
 - If not, the client detects the mapping type as described in step 5.
5. The STUN client uses Endpoint (X:XP) to send a Binding request to Endpoint (Y2:YP2) of the STUN server. The STUN server uses Endpoint (Y2:YP2) to send a Binding response to the STUN client. The Binding response includes the mapped Endpoint (X3:XP3) of the STUN client.
6. After receiving the Binding response, the STUN client checks whether Endpoint (X3:XP3) equals Endpoint (X2:XP2) in step 3.
 - If yes, the client considers that the mapping type is ADM.
 - If not, the client considers that the mapping type is APDM.

Figure 34 Process of NAT mapping type detection



NAT filtering method detection

Suppose the IP address and port number of the STUN server is Y1:YP1, and the alternate IP address and port number of the STUN server is Y2:YP2. The IP address and port number of the STUN client is X:XP.

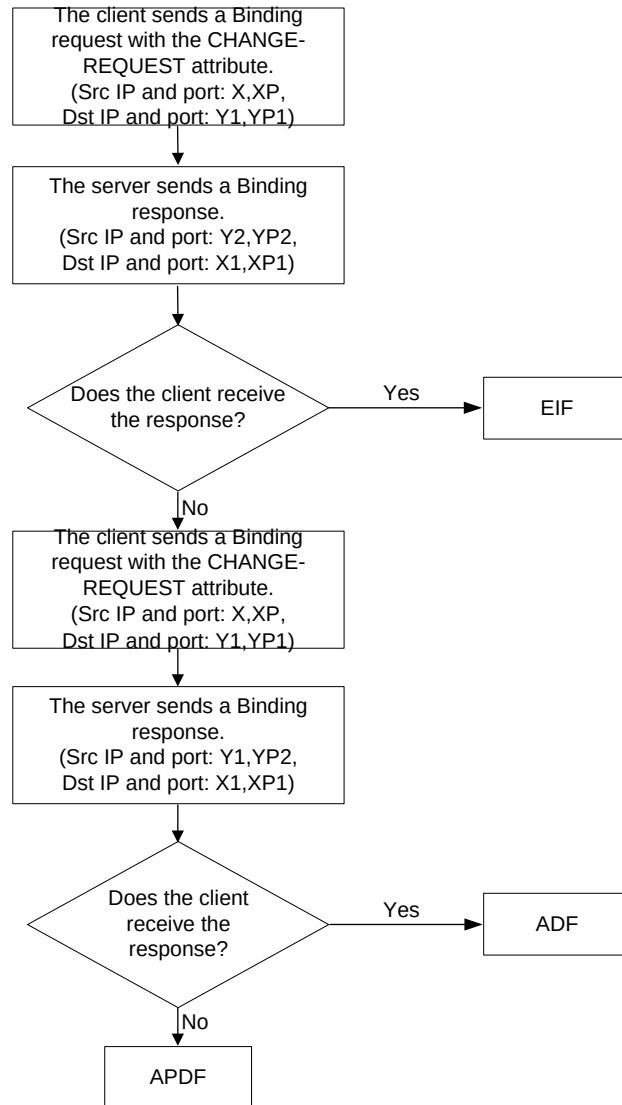
Figure 35 shows the process of NAT filtering method detection.

1. The STUN client sends a Binding request with source IP address and port number Endpoint (X:XP) to Endpoint (Y1:YP1) of the STUN server. The request includes the CHANGE-REQUEST attribute, which requests that the server use a different IP address and port number when sending the response. The OTHER-ADDRESS attribute in the response indicates that the alternate IP address and port number of the STUN server is Endpoint (Y2:YP2). The STUN server uses Endpoint (Y2:YP2) to send a Binding response to the STUN client.
2. If the client receives the Binding response, it considers that the mapping type is EIM.
3. If the client fails to receive the Binding response, it continues to detect the mapping type as described in step 3.
4. The client uses Endpoint (X:XP) to send a Binding request to Endpoint (Y1:YP1) of the STUN server. The request includes the CHANGE-REQUEST attribute, which requests that the server

use a different IP address and port number when sending the response. The OTHER-ADDRESS attribute in the response indicates that the alternate port number of the STUN server is YP2. The STUN server uses Endpoint (Y1,YP2) to send a Binding response to the client.

5. If the client receives the Binding response, it considers that the mapping type is ADF.
6. If the client fails to receive the Binding response, it considers that the mapping type is APDF.

Figure 35 Process of NAT filtering method detection



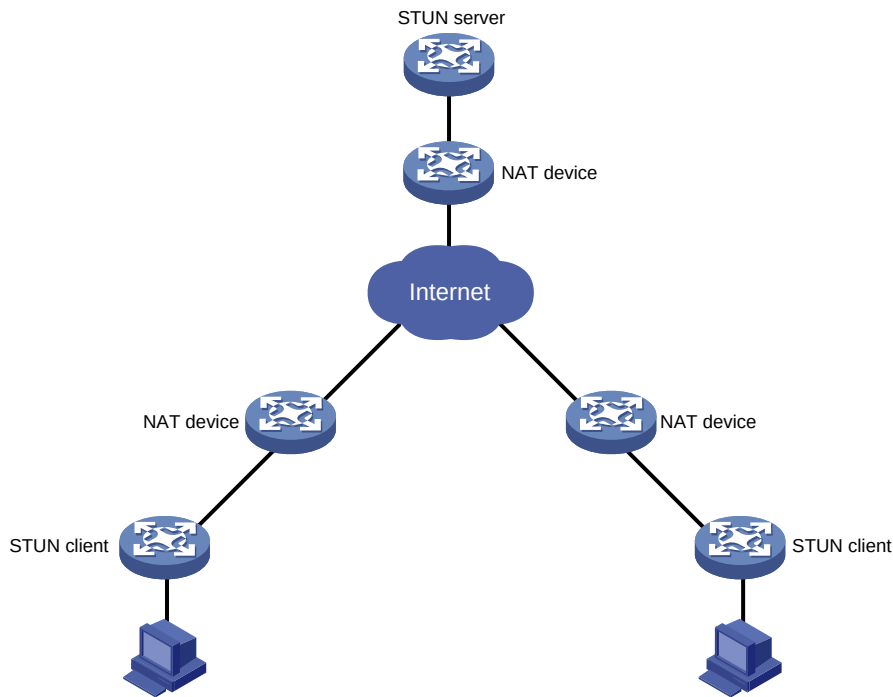
STUN server deployment in private networks

Typically, a STUN server is deployed in a public network. After receiving a Binding request from a STUN client, a STUN server sends a Binding response with the IP address in its payload as the public address of the STUN server. If a STUN server is deployed in a private network, the IP address in the Binding response is the private address of the STUN server. When receiving a subsequent Binding request, the STUN server-side NAT device will not translate the private address in the request to a public address. For STUN to work correctly in this case, perform the following tasks:

- On the STUN server, specify the IP address and alternate IP address of the STUN server after NAT.
- Use one-to-one NAT mapping rule on the NAT device.

In this manner, STUN clients will not sense the private address of the STUN server and uses the public address of the STUN server for communication. The STUN server will still use its public address in Binding responses.

Figure 36 STUN server deployment in a private network



Client retransmissions

STUN runs over UDP, and STUN packets might be discarded during transit. Reliability of STUN request/response transactions is accomplished through retransmissions of the STUN request by the client as follows:

1. The client retransmits a request at an interval if failing to receive a response.
2. The client stops retransmissions until receiving a response or having retransmitted the maximum number of requests.
3. If the client fails to receive a response after the last request is sent, it considers the transaction to have failed.

Protocols and standards

- RFC 3489, *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*
- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*
- RFC 5389, *Session Traversal Utilities for NAT (STUN)*
- RFC 5780, *NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)*

Restrictions and guidelines: STUN configuration

For STUN detection to work correctly, make sure the STUN client can reach both the IP address and alternate IP address of the STUN server.

STUN tasks at a glance

To configure STUN, perform the following tasks:

- [Configure the STUN server](#)
- [Configure the STUN client](#)

Prerequisites for STUN

STUN is used to address NAT traversal in an SDWAN network, and the STUN detection results are transmitted in an SDWAN tunnel. Before you configure STUN, you must configure SDWAN (see *SDWAN Configuration Guide*).

Configure the STUN server

1. Enter system view.
system-view
2. Enable the STUN server and configure an IP address and port number for the STUN server.
stun server ip *ip-address* [**port** *port-number*] [**alternative-ip** *ip-address* [**alternative-port** *port-number*]] [**vpn-instance** *vpn-instance-name*] [**global-ip** *global-ip-address* [**global-port** *port-number*] [**global-alternative-ip** *ip-address* [**global-alternative-port** *port-number*]]]
By default, the STUN server is disabled.

Configure the STUN client

About this task

After you configure this feature on a tunnel interface of the device, the device operates as a STUN client to establish a connection with the specified STUN server. Then, it sends a Binding request to the STUN server. A STUN server and STUN client exchange STUN packets (Binding requests and Binding responses) to detect the IP address and port number assigned by a NAT device and the NAT type.

You can specify multiple STUN servers on the STUN client to perform detection. The STUN client works as follows:

1. The STUN client sends a Binding request to each specified STUN server.
2. The STUN client can process only one Binding response sent from a STUN server at a time. Once the STUN client obtains the NAT type and public IP address and port number after NAT, the detection stops.
3. If the detection fails, the STUN client repeats the above procedure.

Restrictions and guidelines

When you specify multiple STUN servers on a STUN client, make sure the STUN servers are located behind the same NAT device. If the STUN servers are located behind different NAT devices, the detection result might be wrong.

Procedure

1. Enter system view.
system-view
2. Enter tunnel interface view.

```
interface tunnel number [ mode { advpn { gre | udp } [ ipv6 ] | ds-lite-afr | eogre |
eogre-udp | evi [ ipv6 ] | gre [ ipv6 ] | gre-p2mp [ ipv6 ] | ipsec [ ipv6 ] |
ipv4-ipv4 | ipv4-ipv6 | ipv6 | ipv6-ipv4 [ 6rd | 6to4 | auto-tunnel | isatap ] |
ipv6-ipv6 | mgre | mpls-te | nve | nvgre | sdwan udp | sr ipv6 | { vxlan | vxlan-dci }
[ ipv6 ] } ]
```

For more information about this command, see tunneling commands in *Layer 3—IP Services Configuration Guide*.

3. Enable the STUN client on the interface and specify the IP address and port number of the STUN server.

```
stun client destination-ip ip-address [ destination-port port-number ] [ out-interface
interface-type interface-number ]
```

By default, the STUN client is disabled.

Command reference

display stun client info

Use **display stun client info** to display packet statistics and NAT information on the STUN client.

Syntax

```
display stun client info
```

Views

Any view

Predefined user roles

network-admin
network-operator

Examples

Display packet statistics and NAT information on the STUN client.

```
<Sysname> display stun client info
```

```
Totally 1 STUN clients
```

Local IP/port	: 1.1.1.24/6666
Local VPN	: -
NAT IP/port	: 66.1.1.1/6666
NAT type	: Full Cone NAT
STUN refresh times	: 5657
STUN request timeouts	: 2
Basic requests sent	: 11324
Behavior requests sent	: 5517
Filter requests sent	: 5518
Received response to basic requests	: 11315
Received response to behavior requests	: 5517
Received response to filter requests	: 5517
Transaction ID errors in received responses	: 0

Table 53 Command output

Field	Description
Local IP/port	IP address and port number that the STUN client uses for detection.
Local VPN	VPN instance to which the tunnel interface on the STUN client belongs.
NAT IP/port	Public IP address and port number
NAT type	NAT type: • Full Cone NAT. • Restricted Cone NAT. • Port Restricted Cone NAT. • Symmetric NAT. • NO NAT—No NAT device exists. • —Unknown type.
STUN refresh times	Number of times the STUN client refreshes the detection result.
STUN request timeouts	Number of detection timeouts.
Basic requests sent	Number of Basic requests sent. A Basic request is used to detect the public IP address and port number assigned by a NAT device.
Behavior requests sent	Number of Behavior requests sent. A Behavior request is used to detect the NAT mapping type.
Filter requests sent	Number of Filtering requests sent. A Filtering request is used to detect the NAT filtering method.

Related commands**reset stun client statistics****display stun server packet-statistics**

Use **display stun server packet-statistics** to display packet statistics on the STUN server.

Syntax**display stun server packet-statistics****Views**

Any view

Predefined user roles

network-admin

network-operator

Examples

Display packet statistics on the STUN client.

```
<Sysname> display stun server packet-statistics
  STUN success/error requests received  : 22386/0
  STUN success/error responses sent      : 22386/0
  STUN requests dropped                  : 0
  STUN packets received                  : 22386
```

STUN unknown packets received : 0

Table 54 Command output

Field	Description
STUN success/error requests received	Number of success/error requests received by the STUN server.
STUN success/error responses sent	Number of success/error responses sent by the STUN server.
STUN requests dropped	Number of requests dropped by the STUN server.
STUN packets received	Number of packets received by the STUN server.
STUN unknown packets received	Number of unknown packets received by the STUN server.

Related commands

reset stun server packet-statistics

reset stun client statistics

Use **reset stun client statistics** to clear packet statistics on all STUN clients.

Syntax

reset stun client statistics

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command clears packet statistics on all STUN clients. Please use command with caution.

Examples

```
# Clear packet statistics on all STUN clients.  
<Sysname> reset stun client statistics
```

Related commands

display stun client info

reset stun server packet-statistics

Use **reset stun server packet-statistics** to clear packet statistics on all STUN servers.

Syntax

reset stun server packet-statistics

Views

Any view

Predefined user roles

network-admin

Examples

```
# Clear packet statistics on all STUN servers.  
<Sysname> reset stun server packet-statistics
```

Related commands

display stun server packet-statistics

stun client

Use **stun client** to enable the STUN client on an interface and specify the IP address and port number of the STUN server.

Use **undo stun client** to disable the STUN client on an interface or delete the configuration for the specified STUN server.

Syntax

stun client destination-ip *ip-address* [**destination-port** *port-number*] [**out-interface** *interface-type interface-number*]

undo stun client destination-ip [*ip-address*]

Default

The STUN client is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

destination-ip *ip-address*: Specifies the IP address of the STUN server.

destination-port *port-number*: Specifies the port number of the STUN server, in the range of 1024 to 65535. The default is 3478.

out-interface *interface-type interface-number*: Specifies an output interface by its type and number. If you do not specify this option, the STUN client sends packets through the output interface of the route.

Usage guidelines

Application scenarios

STUN uses a client-server model that consists of a STUN client and a STUN server. The STUN server and STUN client exchange STUN packets (Binding requests and Binding responses) to detect the IP address and port number assigned by a NAT device and the NAT type.

Operating mechanism

The STUN client is an entity that sends STUN requests and receives STUN responses. After you execute this command on a tunnel interface of the device, the device operates as a STUN client to establish a connection with the specified STUN server. Then, it sends a Binding request to the STUN server.

You can specify multiple STUN servers on the STUN client to perform detection. The STUN client works as follows:

1. The STUN client sends a Binding request to each specified STUN server.

2. The STUN client can process only one Binding response sent from a STUN server at a time. Once the STUN client obtains the NAT type and public IP address and port number after NAT, the detection stops.
3. If the detection fails, the STUN client repeats the above procedure.

Recommended configuration

In an SDWAN network with multiple WAN interfaces, the NAT type and address translation result might be wrong when you use STUN to detect the IP address and port number after NAT. To avoid such an issue, specify the output interface when you execute the **stun client** command. The specified output interface must be the same as that specified for tunneled packets by using the **tunnel out-interface** command.

Restrictions and guidelines

For the STUN client to establish a connection with a STUN server, do not specify the alternate IP address of the STUN server in this command.

When you specify multiple STUN servers on a STUN client, make sure the STUN servers are located behind the same NAT device. If the STUN servers are located behind different NAT devices, the detection result might be wrong.

When you execute this command, follow these restrictions and guidelines:

- When you execute the **undo stun client destination-ip** command, if you specify the IP address of the STUN server, this command only deletes the configuration for the STUN server. If you do not specify the IP address of the STUN server, this command disables the STUN client.
- To change the IP address and port number of the STUN server specified in this command, you must execute the **undo stun client** command and then specify a new IP address and port number by using the **stun client** command.
- You can specify a maximum of eight STUN servers by repeating this command.

For STUN detection to work correctly, make sure the STUN client can reach both the IP address and alternate IP address of the STUN server.

Examples

Enable the STUN client on SDWAN tunnel interface **Tunnel1** and specify the IP address and port number of the STUN server.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode sdwan udp
[Sysname-Tunnel1] stun client destination-ip 122.225.128.143 destination-port 1025
```

Related commands

tunnel out-interface

stun server

Use **stun server** to enable the STUN server and configure an IP address and port number for the STUN server.

Use **undo stun server** to disable the STUN server.

Syntax

```
stun server ip ip-address [ port port-number ] [ alternative-ip ip-address [ alternative-port port-number ] ] [ vpn-instance vpn-instance-name ] [ global-ip global-ip-address [ global-port port-number ] [ global-alternative-ip ip-address [ global-alternative-port port-number ] ] ]
```

undo stun server ip *ip-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

Default

The STUN server is disabled.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

ip *ip-address*: Specifies an IP address for the STUN server.

port *port-number*: Specifies a port number for the STUN server, in the range of 1024 to 65535. The default is 3478.

alternative-ip *ip-address*: Specifies an alternate IP address for the STUN server.

alternative-port *port-number*: Specifies an alternate port number for the STUN server, in the range of 1024 to 65535. The default is 3479. If do not specify this option for a STUN server that is deployed in the public network, the STUN client cannot determine the NAT type.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the STUN server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the STUN server belongs to the public network, do not specify this option.

global-ip *ip-address*: Specifies the public IP address for the STUN server after NAT.

global-port *port-number*: Specifies the public port number for the STUN server after NAT, in the range of 1024 to 65535.

global-alternative-ip *ip-address*: Specifies the alternate public IP address for the STUN server after NAT. If do not specify this option for a STUN server that is deployed in a private network, the STUN client cannot determine the NAT type.

global-alternative-port *port-number*: Specifies the alternate public port number for the STUN server after NAT, in the range of 1024 to 65535.

Usage guidelines

Typically deployed on the public network, the STUN server is an entity that receives STUN requests and sends STUN responses. The STUN server and STUN client exchange STUN packets to detect the IP address and port number assigned by a NAT device and the NAT type.

If a STUN server is deployed in a private network and communicates with the public network through a NAT device configured with a one-to-one NAT mapping rule, the STUN server uses its private address as the IP address in Binding responses. When receiving a subsequent Binding request, the STUN server-side NAT device will not translate the private address in the request to a public address, which leads to STUN detection failure.

To solve the problem, specify the **global-ip** *global-ip-address* and **global-alternative-ip** *ip-address* parameters. The STUN server will use the specified public address in Binding responses it sends. The specified public addresses must match the public IP addresses on the NAT device.

In a multi-egress environment, you can execute this command multiple times to configure multiple STUN servers.

For STUN detection to work correctly, make sure the STUN client can reach both the IP address and alternate IP address of the STUN server. To change the IP address and port number of the STUN server configured in this command, you must execute the **undo stun server** command and then configure a new IP address and port number by using the **stun server** command.

In the public network or in the same VPN instance:

- Any two IP addresses of a STUN server must be different. Any IP address of a STUN server cannot be the same as any IP address of another STUN server.
- The port number and alternate port number of the same STUN server cannot be the same. The public port number or alternate public port number of a STUN server cannot be the same as the public port number or alternate public port number of another STUN server.

As a best practice, execute the **display udp** command to obtain the value for the **Local Addr:port** field before you configure a STUN server. The **Local Addr:port** field represents the local IPv4 addresses and port numbers that are being used. To deploy configuration successfully, do not specify a used local port number for the STUN server.

Examples

Enable the STUN server and configure an IP address and port number and an alternate IP address and port number for the STUN server.

```
<Sysname> system-view
```

```
[Sysname] stun server ip 10.1.1.1 port 4396 alternative-ip 20.1.1.1 alternative-port 4397
```

Related commands

display udp

New feature: Cloud connections

About cloud connections

A cloud connection is a management tunnel established between a local device and the cloud server. It enables you to manage the local device from the cloud server without accessing the network where the device resides.

Multiple subconnections

After a local device establishes a connection with the cloud server, service modules on the local device can establish multiple subconnections with the microservices on the cloud server. These subconnections are independent from each other and provide separate communication channels for different services. This mechanism avoids interference among different services.

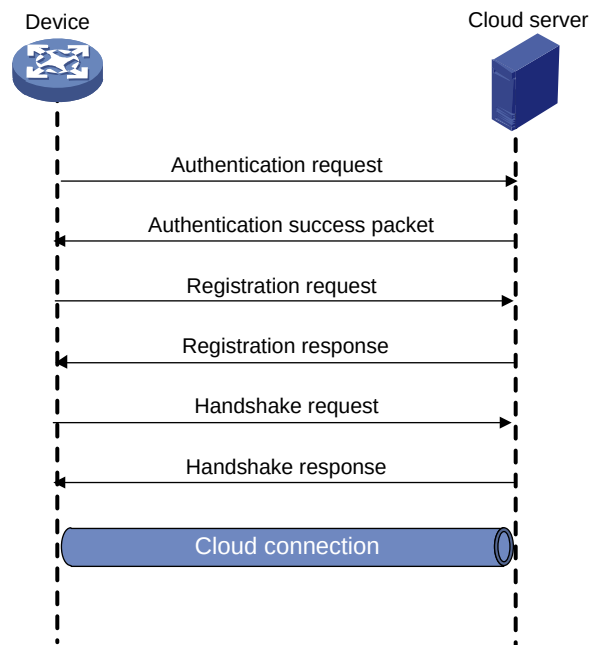
Cloud connection establishment

As shown, the cloud connection between the device and the cloud server is established as follows:

1. The device sends an authentication request to the cloud server.
2. The cloud server sends an authentication success packet to the device.
The device passes the authentication only if the serial number of the device has been added to the cloud server. If the authentication fails, the cloud server sends an authentication failure packet to the device.
3. The device sends a registration request to the cloud server.
4. The cloud server sends a registration response to the device.
The registration response contains the uniform resource locator (URL) used to establish a cloud connection.
5. The device uses the URL to send a handshake request (changing the protocol from HTTP to WebSocket) to the cloud server.

6. The cloud server sends a handshake response to the device to finish establishing the cloud connection.
7. After the cloud connection is established, the device automatically obtains the subconnection URLs and establishes subconnections with the cloud server based on the service needs.

Figure 37 Establishing a cloud connection



Configuring the cloud server

For a successful cloud connection establishment, add the serial number of the device to be managed to the cloud server. For more information about the cloud server settings, see the installation guide for the cloud server.

Configuring the local device

About this task

You can specify a cloud server by its domain name and log in to the server through the domain name on a remote PC to manage the local device.

For a device to establish a cloud connection to the cloud server, perform either of the following tasks:

- Specify the domain name of the cloud server on the device through CLI.
- Configure VLAN interface 1 of the device as a DHCP client and the cloud server as the DHCP server. The device obtains the IP address of the DHCP server and parses the option 253 field in the DHCP packets to obtain the domain name of the cloud server. When the domain name obtained through the option 253 field is an IPv4 or IPv6 address, the device uses the IPv4 or IPv6 address to connect to the cloud server. When the domain name obtained through the option 253 field is not an IPv4 or IPv6 address, the device parses the domain name into an IPv4 address. If the device fails to parse the domain name into an IPv4 address, it will not parse the domain name into an IPv6 address. For more information about the option 253 field, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

To establish cloud connections to the cloud server, a password is required. A device can use either of the following methods to obtain the password for establishing cloud connections to the cloud server:

- Execute the **cloud-management server password** command on the device to specify the password for establishing cloud connections to the cloud server.
- Configure VLAN interface 1 of the device as a DHCP client and the cloud server as the DHCP server. The device obtains the IP address of the DHCP server and parses the option 252 field in the DHCP packets to obtain the password for connection to the cloud server. For more information about the option 252 field, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

After establishing the cloud connection, the local device sends keepalive packets to the cloud server at the interval specified by the **cloud-management keepalive interval** command. If the device does not receive a response from the cloud server after the number of keepalive packets sent reached the limit specified by the **cloud-management keepalive count count** command, the device sends a registration request to re-establish the cloud connection.

To prevent NAT entry aging, the local device sends ping packets to the cloud server periodically.

If the cloud server verifies the token of a device before establishing a cloud connection to the device, you must configure the token on the device. To avoid authentication failure, make sure the token configured on the device is consistent with that specified for the device on the cloud server.

Restrictions and guidelines

You can specify one primary server by using the **cloud-management server domain** command and a maximum of eight IPv4 and IPv6 backup servers by repeating the **cloud-management backup-server domain** command. Each server domain name supports a maximum of three port numbers.

When establishing a cloud connection, the device can connect to only one cloud server at one time according to the sequence in which the servers are stored. The server domain names are stored in alphabet order and port numbers are in descending order. To view the connected server, execute the **display cloud-management state** command.

If multiple servers exist in the intranet and the NAT device has only one public IP address, you can execute this command to specify different port numbers for one server domain name.

When establishing a cloud connection, the first specified server has the highest priority. When the connected server fails, the device switches to another server and does not switch back to the original server even if the original server recovers.

The domain name obtained through DHCP has a higher priority than the domain name configured manually.

If a device obtains the domain name of the cloud server through DHCP after establishing a cloud connection to the cloud server with the manually configured domain name, the device performs the following tasks:

- If the automatically obtained and manually configured domain names are identical, the device retains the cloud connection.
- If the automatically obtained and manually configured domain names are different, the device tears down the cloud connection and then establishes a cloud connection to the cloud server with the automatically obtained domain name.

The password obtained through DHCP has a higher priority than the password configured manually.

If a device obtains the password for connection to the cloud server through DHCP after establishing a cloud connection to the cloud server with the manually configured password, the device performs the following tasks:

- If the automatically obtained and manually configured passwords are identical, the device retains the cloud connection.
- If the automatically obtained and manually configured passwords are different, the device tears down the cloud connection and then establishes a cloud connection to the cloud server with the automatically obtained password.

Reduce the ping interval value if the network condition is poor or the NAT entry aging time is short. When you use the cloud server for cloud connections, you must set the password for establishing cloud connections to the cloud server.

Prerequisites

Before configuring this feature, make sure a DNS server is configured to translate domain names.

To obtain the domain name of the cloud server automatically, first configure the option 253 field as the domain name of the cloud server.

To obtain the password for connection to the cloud server automatically, first configure the option 252 field as the password of the cloud server.

Procedure

1. Enter system view.

system-view

2. Specify the primary cloud server by its domain name.

cloud-management server [**ipv6**] **domain** *domain-name* [**port** *port-number*]
[**vpn-instance** *vpn-instance-name*] [**source-ip** *ip-address*]

By default, no primary cloud server is specified.

3. (Optional.) Specify the domain name of a backup cloud server.

cloud-management backup-server [**ipv6**] **domain** *domain-name* [**port** *port-number*]
[**vpn-instance** *vpn-instance-name*] [**source-ip** *ip-address*]

By default, no backup cloud server is specified

4. (Optional.) Set the keepalive interval.

cloud-management keepalive *interval*

By default, the keepalive interval is 180 seconds.

5. (Optional.) Specify the maximum number of consecutive keepalive packets that the local device can send to the cloud server.

cloud-management keepalive count *count*

By default, the local device can send three consecutive keepalive packets to the cloud server.

6. (Optional.) Set the ping interval.

cloud-management ping *interval*

By default, the ping interval is 60 seconds.

7. (Optional.) Specify the TCP port number used by the device to initiate the authentication to the cloud server.

cloud-management server port *port-number*

By default, TCP port number 19443 is used by the device to initiate the authentication to a cloud server.

8. (Optional.) Set the password for establishing cloud connections to the cloud server.

cloud-management server password { **cipher** | **simple** } *string*

By default, no password is set for establishing cloud connections to the cloud server.

9. (Optional.) Set the token for establishing cloud connections to the cloud server.

cloud-management token { **cipher** | **simple** } *string*

By default, no token is set for establishing cloud connections to the cloud server.

Unbinding the device from the cloud server

About this task

A device can be registered on the cloud server by only one user.

To register a device that has been registered by another user, you need to take the following steps:

1. Obtain a verification code for device unbinding from the cloud server.
2. Execute the command on the device for sending the verification code to the cloud server.
3. Register the device on the cloud server.

Procedure

1. Enter system view.
system-view
2. Send the verification code for device unbinding to the cloud server.
cloud-management unbinding-code *code*

Command reference

cloud-management backup-server domain

Use **cloud-management backup-server domain** to specify the domain name of a backup cloud server.

Use **undo cloud-management backup-server domain** to remove one or all backup cloud servers.

Syntax

```
cloud-management backup-server [ ipv6 ] domain domain-name [ port port-number ]  
[ vpn-instance vpn-instance-name ] [ source-ip ip-address ]  
  
undo cloud-management backup-server [ ipv6 ] domain [ domain-name [ port  
port-number ] ]
```

Default

No backup cloud server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 backup cloud server. If you do not specify this keyword, the command specifies an IPv4 backup cloud server.

domain-name: Specifies a backup cloud server by its domain name, a case-insensitive string of 1 to 253 characters. If you do not specify this parameter in the **undo cloud-management backup-server domain** command, all backup cloud servers will be deleted.

port port-number: Specifies the TCP port number used by the device to initiate the authentication to the backup cloud server. The value range is 1 to 65535. If you do not specify this option, this command uses the port number specified by the **cloud-management server port** command.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the backup cloud server is on the public network.

source-ip *ip-address*: Specifies the source IP address for the device that connects to the backup cloud server. It must be the same as the IP address configured on the device. If you do not specify this option, the device uses the primary IP address of the egress interface to connect to the backup cloud server.

Usage guidelines

Before configuring this command, make sure a DNS server is configured to translate domain names.

You can specify a maximum of eight IPv4 and IPv6 backup servers by repeating the **cloud-management backup-server domain** command. Each server domain name supports a maximum of three port numbers. If you execute this command multiple times to configure a backup cloud server with the same domain name and the same port number, the most recent configuration takes effect.

When establishing a cloud connection, the device can connect to only one cloud server at one time according to the sequence in which the servers are stored. The server domain names are stored in alphabet order and port numbers are in descending order. To view the connected server, execute the **display cloud-management state** command.

If multiple servers exist in the intranet and the NAT device has only one public IP address, you can execute this command to specify different port numbers for one server domain name.

When establishing a cloud connection, the first specified server has the highest priority. When the connected server fails, the device switches to another server and does not switch back to the original server even if the original server recovers.

For a device to establish a cloud connection to the cloud server, perform either of the following tasks:

- Specify the domain name of the cloud server on the device through CLI.
- Configure VLAN interface 1 of the device as a DHCP client and the cloud server as the DHCP server. The device obtains the IP address of the DHCP server and parses the option 253 field in the DHCP packets to obtain the domain name of the cloud server. When the domain name obtained through the option 253 field is an IPv4 or IPv6 address, the device uses the IPv4 or IPv6 address to connect to the cloud server. When the domain name obtained through the option 253 field is not an IPv4 or IPv6 address, the device parses the domain name into an IPv4 address. If the device fails to parse the domain name into an IPv4 address, it will not parse the domain name into an IPv6 address. For more information about the option 253 field, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

The domain name obtained through DHCP has a higher priority than the domain name configured manually.

If a device obtains the domain name of the cloud server through DHCP after establishing a cloud connection to the cloud server with the manually configured domain name, the device performs the following tasks:

- If the automatically obtained and manually configured domain names are identical, the device retains the cloud connection.
- If the automatically obtained and manually configured domain names are different, the device tears down the cloud connection and then establishes a cloud connection to the cloud server with the automatically obtained domain name.

Examples

Specify the server with domain name **123.com** and port number 10001 as an IPv4 backup cloud server.

```
<Sysname> system-view
```

```
[Sysname] cloud-management backup-server domain 123.com port 10001
```

Related commands

display cloud-management state

cloud-management keepalive

Use **cloud-management keepalive** to set the keepalive interval for the local device to send keepalive packets to the cloud server.

Use **undo cloud-management keepalive** to restore the default.

Syntax

cloud-management keepalive *interval*

undo cloud-management keepalive

Default

The keepalive interval is 180 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the keepalive interval in the range of 10 to 600 seconds.

Usage guidelines

After establishing the cloud connection, the local device sends keepalive packets to the cloud server at the interval specified by the **cloud-management keepalive** *interval* command. If the device does not receive a response from the cloud server after the number of keepalive packets sent reached the limit specified by the **cloud-management keepalive count** *count* command, the device sends a registration request to re-establish the cloud connection.

Examples

```
# Set the keepalive interval to 360 seconds.  
<Sysname> system-view  
[Sysname] cloud-management keepalive 360
```

Related commands

cloud-management keepalive count

cloud-management keepalive count

Use **cloud-management keepalive count** to specify the maximum number of consecutive keepalive packets that the local device can send to the cloud server.

Use **undo cloud-management keepalive count** to restore the default.

Syntax

cloud-management keepalive count *count*

undo cloud-management keepalive count

Default

A device can send three consecutive keepalive packets to the cloud server.

Views

System view

Predefined user roles

network-admin

Parameters

count: Specifies the maximum number of consecutive keepalive packets that the local device can send to the cloud server. The value range for this argument is 2 to 100.

Usage guidelines

After establishing the cloud connection, the local device sends keepalive packets to the cloud server at the interval specified by the **cloud-management keepalive interval** command. If the device does not receive a response from the cloud server after the number of keepalive packets sent reached the limit specified by the **cloud-management keepalive count count** command, the device sends a registration request to re-establish the cloud connection.

Examples

Set the maximum number of consecutive keepalive packets that the local device can send to the cloud server to 5.

```
<Sysname> system-view
```

```
[Sysname] cloud-management keepalive count 5
```

Related commands

cloud-management keepalive

cloud-management ping

Use **cloud-management ping** to set the interval at which the local device sends ping packets to the cloud server.

Use **undo cloud-management ping** to restore the default.

Syntax

cloud-management ping interval

undo cloud-management ping

Default

The local device sends ping packets to the cloud server at intervals of 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which the local device sends ping packets to the cloud server, in the range of 10 to 600 seconds.

Usage guidelines

After the connection to the cloud server is established, the local device sends ping packets to the server periodically to prevent NAT entry aging. Reduce the interval value if the network condition is poor or the NAT entry aging time is short.

The cloud server does not respond to ping packets.

Examples

```
# Configure the local device to send ping packets to the cloud server at intervals of 120 seconds.
<Sysname> system-view
[Sysname] cloud-management ping 120
```

cloud-management server domain

Use **cloud-management server domain** to specify the primary cloud server by its domain name.

Use **undo cloud-management server domain** to restore the default.

Syntax

```
cloud-management server [ ipv6 ] domain domain-name [ port port-number ]
[ vpn-instance vpn-instance-name ] [ source-ip ip-address ]
```

```
undo cloud-management server domain
```

Default

No primary cloud server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 primary cloud server. If you do not specify this keyword, the command specifies an IPv4 primary cloud server.

domain-name: Specifies the primary cloud server by its domain name, a case-insensitive string of 1 to 253 characters.

port port-number: Specifies the TCP port number used by the device to initiate the authentication to the primary cloud server. The value range is 1 to 65535. If you do not specify this option, this command uses the port number specified by the **cloud-management server port** command.

vpn-instance vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the primary cloud server is on the public network.

source-ip ip-address: Specifies the source IP address for the device that connects to the primary cloud server. It must be the same as the IP address configured on the device. If you do not specify this option, the device uses the primary IP address of the egress interface to connect to the primary cloud server.

Usage guidelines

Before configuring this command, make sure a DNS server is configured to translate domain names.

Only one primary cloud server is supported. If you execute the command multiple times, the most recent configuration takes effect.

If multiple servers exist in the intranet and the NAT device has only one public IP address, you can execute this command to specify different port numbers for one server domain name.

For a device to establish a cloud connection to the cloud server, perform either of the following tasks:

- Specify the domain name of the cloud server on the device through CLI.
- Configure VLAN interface 1 of the device as a DHCP client and the cloud server as the DHCP server. The device obtains the IP address of the DHCP server and parses the option 253 field in the DHCP packets to

obtain the domain name of the cloud server. When the domain name obtained through the option 253 field is an IPv4 or IPv6 address, the device uses the IPv4 or IPv6 address to connect to the cloud server. When the domain name obtained through the option 253 field is not an IPv4 or IPv6 address, the device parses the domain name into an IPv4 address. If the device fails to parse the domain name into an IPv4 address, it will not parse the domain name into an IPv6 address. For more information about the option 253 field, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

The domain name obtained through DHCP has a higher priority than the domain name configured manually.

If a device obtains the domain name of the cloud server through DHCP after establishing a cloud connection to the cloud server with the manually configured domain name, the device performs the following tasks:

- If the automatically obtained and manually configured domain names are identical, the device retains the cloud connection.
- If the automatically obtained and manually configured domain names are different, the device tears down the cloud connection and then establishes a cloud connection to the cloud server with the automatically obtained domain name.

Examples

```
# Specify the server with domain name abc.com and port number 10001 as the IPv4 primary cloud server.
```

```
<Sysname> system-view
```

```
[Sysname] cloud-management server domain abc.com port 10001
```

Related commands

display cloud-management state

cloud-management server password

Use **cloud-management server password** to set the password for establishing cloud connections to the cloud server.

Use **cloud-management server password** to restore the default.

Syntax

cloud-management server password { cipher | simple } string

undo cloud-management server password

Default

No password is set for establishing cloud connections to the cloud server.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies the password in encrypted form.

simple: Specifies the password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. The plaintext form is a case-sensitive string of 1 to 63 characters. The encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

After you change the password, the device terminates the cloud connections that have been established (if any) and uses the new password to establish cloud connections.

A device can use either of the following methods to obtain the password for establishing cloud connections to the cloud server:

- Execute this command on the device to specify the password for establishing cloud connections to the cloud server.
- Configure VLAN interface 1 of the device as a DHCP client and the cloud server as the DHCP server. The device obtains the IP address of the DHCP server and parses the option 252 field in the DHCP packets to obtain the password for connection to the cloud server. For more information about the option 252 field, see DHCP configuration in *Layer 3—IP Services Configuration Guide*.

The password obtained through DHCP has a higher priority than the password configured manually.

If a device obtains the password for connection to the cloud server through DHCP after establishing a cloud connection to the cloud server with the manually configured password, the device performs the following tasks:

- If the automatically obtained and manually configured passwords are identical, the device retains the cloud connection.
- If the automatically obtained and manually configured passwords are different, the device tears down the cloud connection and then establishes a cloud connection to the cloud server with the automatically obtained password.

Examples

```
# Set the password for establishing cloud connections to the cloud server to 12345678 in plaintext format.
```

```
<Sysname> system-view
```

```
[Sysname] cloud-management server password simple 12345678
```

cloud-management server port

Use **cloud-management server port** to specify the TCP port number used by the device to initiate the authentication to a cloud server.

Use **undo cloud-management server port** to restore the default.

Syntax

cloud-management server port *port-number*

undo cloud-management server port

Default

TCP port number 19443 is used by the device to initiate the authentication to a cloud server.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a TCP port number used by the device to initiate the authentication to a cloud server. The value range is 1 to 65535.

Usage guidelines

If you configure the primary cloud server or a backup cloud server without specifying a TCP port number, the device uses the port number specified by this command to initiate the authentication to a cloud server.

Examples

```
# Specify the TCP port number used by the device to initiate the authentication to a cloud server as 80.
<Sysname> system-view
[Sysname] cloud-management server port 80
```

Related commands

display cloud-management state

cloud-management token

Use **cloud-management token** to set the token for establishing cloud connections to the cloud server.

Use **undo cloud-management token** to restore the default.

Syntax

```
cloud-management token { cipher | simple } string
undo cloud-management token
```

Default

No token is set for establishing cloud connections to the cloud server.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies the token in cipher text.

simple: Specifies the token in plain text. The token will be stored in cipher text for security purposes.

string: Specifies the token string. The token in plain text form is a case-sensitive string of 1 to 63 characters. The token in cipher text form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

If the cloud server verifies the token of a device before establishing a cloud connection to the device, you must configure the token on the device. To avoid authentication failure, make sure the token configured on the device is consistent with that specified for the device on the cloud server.

After you change the token, the device terminates the cloud connections that have been established (if any) and uses the new token to re-establish cloud connections.

Examples

```
# Set the token for establishing cloud connections to 12345678 in plain text form.
<Sysname> system-view
[Sysname] cloud-management token simple 12345678
```

cloud-management unbinding-code

Use **cloud-management unbinding-code** to send the verification code for device unbinding to the cloud server.

Syntax

cloud-management unbinding-code *code*

Views

System view

Predefined user roles

network-admin

Parameters

code: Specifies the verification code obtained from the cloud server. The verification code is a case-sensitive string of 16 characters.

Usage guidelines

A device can be registered on the cloud server by only one user.

To register a device that has been registered by another user, you need to take the following steps:

1. Obtain a verification code for device unbinding from the cloud server.
2. Execute this command on the device to send the verification code to the cloud server.
3. Register the device on the cloud server.

Examples

```
# Send the verification code for device unbinding to the cloud server.  
[Sysname] cloud-management unbinding-code A6B9C3C2D5A8Z1S7
```

Related commands

cloud-management server domain

display cloud-management state

Use **display cloud-management state** to display cloud connection state information.

Syntax

display cloud-management state

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

NOTE:

The cloud server domain name and IP address in this example are for illustration only.

```
# Display cloud connection state information.
```

```

<Sysname> display cloud-management state
Cloud connection state           : Established
Device state                     : Request_success
Cloud server address             : 101.36.161.141
Cloud server domain name        : oasis.h3c.com
Cloud connection mode           : Https
Cloud server authentication port : 19443
Cloud server connection port    : 443
Connected at                    : Wed Jan 27 14:18:40 2018
Duration                        : 00d 00h 02m 01s
Process state                   : Message received
Failure reason                  : N/A
Last down reason                : socket connection error (Details:N/A)
Last down at                   : Wed Jan 27 13:18:40 2018
Last report failure reason      : N/A
Last report failure at         : N/A
Dropped packets after reaching buffer limit : 0
Total dropped packets           : 1
Last report incomplete reason   : N/A
Last report incomplete at      : N/A
Buffer full count               : 0

```

Table 55 Command output

Field	Description
Cloud connection state	Cloud connection state: Unconnected , Request , and Established .
Device state	Local device state: • Idle—In idle state. • Connecting—Connecting to the cloud server. • Request_CAS_url—Sent a central authentication service (CAS) URL request. • Request_CAS_url_success—Requesting CAS URL succeeded. • Request_CAS_TGT—Sent a ticket granting ticket (TGT) request. • Request_CAS_TGT_success—Requesting TGT succeeded. • Request_CAS_ST—Sent a service ticket (ST) request. • Request_CAS_ST_success—Requesting ST succeeded. • Request_cloud_auth—Sent an authentication request. • Request_cloud_auth_success—Authentication succeeded. • Register—Sent a registration request. • Register_success—Registration succeeded. • Request—Sent a handshake request. • Request_success—Handshake succeeded.
Cloud server address	IP address of the cloud server.
Cloud server domain name	Domain name of the cloud server.
Cloud server authentication port	TCP port number used by the device to initiate the authentication to a cloud server.
Cloud server	TCP port number used to establish cloud connections.

Field	Description
connection port	
Connected at	Time when the cloud connection was established.
Duration	Duration since the establishment of the cloud connection.
Process state	Cloud connection processing state: • DNS not parsed. • DNS parsed. • Message not sent. • Message sent. • Message not received. • Message received.
Failure reason	Cloud connection failure reason: • DNS parse failed. • Socket connection failed. • SSL creation failed. • Sending CAS url request failed. • Sending CAS TGT failed. • Sending CAS ST failed. • Sending cloud auth failed. • Sending register failed. • Processing CAS url response failed. • Processing CAS TGT response failed. • Processing CAS ST response failed. • Processing cloud auth response failed. • Processing register response failed. • Sending handshake request failed. • Processing handshake failed. • Sending websocket request failed. • Processing websocket packet failed.
Last down reason	Reason for the most recent cloud connection interruption: • Device or process rebooted. • Socket connection error. • Configuration changed. • Received websocket close packet from cloud. • Keepalive expired. • Packet processing failed. • Main connection went down. • Cloud reset connection. • Memory reached threshold.
Last down at	Time when the cloud connection went down most recently.
Last report failure reason	Reason for the most recent cloud connection packet sending failure: • Tunnel is being deleted. • Tunnel socket is invalid. • Failed to convert string to json. • Failed to convert json to string. • Failed to create message node. • Tunnel is not ready. • Failed to create packet buffer. • SSL sending failure.

Field	Description
	If the reason is SSL sending failure, one of the following detailed reason will be displayed: • ssl error none. • ssl error ssl. • ssl error read. • ssl error write. • ssl error x509 lookup. • ssl error syscall. • ssl error zero return. • ssl error connect. • ssl error accept.
Last report failure at	Time when the most recent cloud connection packet sending failure occurred.
Dropped packets after reaching buffer limit	Number of packets that are dropped because the CMTNL buffer limit is reached.
Total dropped packets	Total number of dropped packets.
Last report incomplete reason	Reason for the most recent unfinished packet sending: • Interrupted system call. • Socket buffer is full.
Last report incomplete at	Time when the most recent unfinished packet sending occurred.
Buffer full count	Number of times that the buffer becomes full.

New feature: Specifying a CWMP NTP server

Configuring NTP in client/server mode

Restrictions and guidelines

To configure NTP in client/server mode, specify an NTP server for the client.

For a client to synchronize to an NTP server, make sure the server is synchronized by other devices or uses its local clock as the reference source.

If the stratum level of a server is higher than or equal to a client, the client will not synchronize to that server.

You can specify multiple servers for a client by executing the **ntp-service unicast-server** or **ntp-service ipv6 unicast-server** command multiple times.

Procedure

1. Enter system view.
system-view
2. Specify an NTP server for the device.
IPv4:

ntp-service unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

IPv6:

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

By default, no NTP server is specified.

3. Specify a CWMP NTP server.

ntp-service cwmp unicast-server { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } { **first** | **second** | **third** | **fourth** | **fifth** }

By default, no CWMP NTP servers are configured.

Typically, you can use the **ntp-service unicast-server** command to specify NTP servers for the device. To use CWMP NTP server 1, CWMP NTP server 2, CWMP NTP server 3, CWMP NTP server 4, or CWMP NTP server 5, execute the **ntp-service cwmp unicast-server** command. You cannot use the two commands to specify a same NTP server.

Command reference

ntp-service cwmp unicast-server

Use **ntp-service cwmp unicast-server** to specify a CPE WAN Management Protocol, (CWMP, also called TR-069) NTP server.

Use **undo ntp-service cwmp unicast-server** to delete a CWMP NTP server.

Syntax

ntp-service cwmp unicast-server { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } { **first** | **second** | **third** | **fourth** | **fifth** }

undo ntp-service cwmp unicast-server { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No CWMP NTP servers are configured.

Views

System view

Predefined user roles

network-admin

Parameters

host-name: Specify an NTP server by its host name, a case-sensitive string of 1 to 64 characters. The host name can contain only letters, digits, hyphens (-), underscores (_), and dots (.)

ipv4-address: Specify an NTP server by its IPv4 address. This address can only be a unicast address, and cannot be a broadcast address, multicast address, or IP address of the local clock.

ipv6 *ipv6-address*: Specify an NTP server by its IPv6 address. This address can only be a global unicast address and cannot be a multicast address.

{ **first** | **second** | **third** | **fourth** | **fifth** }: Represents CWMP NTP server 1, CWMP NTP server 2, CWMP NTP server 3, CWMP NTP server 4, and CWMP NTP server 5, respectively. You can

configure a maximum of five CWMP NTP servers for the device. The server numbers does not represent the order of precedence.

Usage guidelines

After you specify an NTP server for the device, the device can synchronize the time with the server, but the server will not synchronize the time with the device.

You can use the **ntp-service cwmp unicast-server** or **ntp-service unicast-server** command to specify NTP servers for the device. When multiple NTP servers are specified for the device and the device receives NTP response messages from multiple NTP servers, the device selects a best clock from the servers based on parameters such as stratum level and synchronizes the time with the best clock.

Typically, you can use the **ntp-service unicast-server** command to specify NTP servers for the device. To use CWMP NTP server 1, CWMP NTP server 2, CWMP NTP server 3, CWMP NTP server 4, or CWMP NTP server 5, use the **ntp-service cwmp unicast-server** command. You cannot use the two commands to specify a same NTP server.

You can execute this command multiple times to specify a maximum of five CWMP NTP servers for the device.

Examples

Specify the server at 1.1.1.1 as CWMP NTP Server 1 and the server at 2.2.2.2 as CWMP NTP Server 2.

```
<Sysname> system-view
[Sysname] ntp-service cwmp unicast-server 1.1.1.1 first
[Sysname] ntp-service cwmp unicast-server 2.2.2.2 second
```

Related commands

ntp-service unicast-server

New feature: Enabling route advertisement for IPv6 prefixes assigned to directly connected clients

Enabling route advertisement for IPv6 prefixes assigned to directly connected clients

About this task

A DHCPv6 client can obtain an IPv6 prefix through DHCPv6 and use this IPv6 prefix to assign IPv6 addresses to hosts in a downstream network. A host in the downstream network cannot access the external network if the following conditions exist:

- The DHCPv6 client is directly connected to the DHCPv6 server, but the client does not run on the same subnet as the host.
- The network-side device does not have a route to the host.

To resolve this issue, use this feature on the DHCPv6 server. This feature enables the DHCPv6 server to generate a routing entry for the IPv6 prefix and advertises this entry to the dynamic routing protocol. When the external network device learns this route through the dynamic routing protocol, it can communicate with the hosts in the downstream network.

Procedure

1. Enter system view.

system-view

2. Enable the DHCPv6 server to advertise routes for the IPv6 prefixes assigned to directly connected clients.

ipv6 dhcp advertise pd-route

By default, the DHCPv6 server does not advertise routes for the IPv6 prefixes assigned to directly connected clients.

Command reference

ipv6 dhcp advertise pd-route

Use **ipv6 dhcp advertise pd-route** to enable the DHCPv6 server to advertise routes for the IPv6 prefixes assigned to directly connected clients.

Use **undo ipv6 dhcp advertise pd-route** to disable the DHCPv6 server from advertising routes for the IPv6 prefixes assigned to directly connected clients.

Syntax

ipv6 dhcp advertise pd-route

undo ipv6 dhcp advertise pd-route

Default

The DHCPv6 server does not advertise routes for the IPv6 prefixes assigned to directly connected clients.

Views

System view

Predefined user roles

network-admin

Usage guidelines

A DHCPv6 client can obtain an IPv6 prefix through DHCPv6 and use this IPv6 prefix to assign IPv6 addresses to hosts in a downstream network. A host in the downstream network cannot access the external network if the following conditions exist:

- The DHCPv6 client is directly connected to the DHCPv6 server, but the client does not run on the same subnet as the host.
- The network-side device does not have a route to the host.

To resolve this issue, use this feature on the DHCPv6 server. This feature enables the DHCPv6 server to generate a routing entry for the IPv6 prefix and advertises this entry to the dynamic routing protocol. When the external network device learns this route through the dynamic routing protocol, it can communicate with the hosts in the downstream network.

To prevent the network-side device from accessing the hosts in downstream network, disable this feature.

Examples

Enable the DHCPv6 server from advertising routes for the IPv6 prefixes assigned to directly connected clients.

```
<Sysname> system-view
[Sysname] ipv6 dhcp advertise pd-route
```


New feature: Enabling the DHCPv6 relay agent to support Option 79

Enabling the DHCPv6 relay agent to support Option 79

About this task

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Enable the DHCPv6 relay agent to support Option 79.
ipv6 dhcp relay client-link-address enable
By default, the DHCPv6 relay agent does not support Option 79.

Command reference

Use **ipv6 dhcp relay client-link-address enable** to enable the DHCPv6 relay agent to support Option 79.

Use **undo ipv6 dhcp relay client-link-address enable** to disable Option 79 support.

Syntax

ipv6 dhcp relay client-link-address enable
undo ipv6 dhcp relay client-link-address enable

Default

The DHCPv6 relay agent does not support Option 79.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If DHCPv6 relay agents exist in the network, the DHCPv6 server needs the MAC address of the DHCPv6 client for authentication or for IPv6 address or prefix assignment. To meet the requirement, enable the DHCPv6 relay agent that the client first passes to support Option 79. This feature allows the DHCPv6 relay agent to learn the MAC address in the client request. When the relay agent generates a Relay-Forward packet for the request, it fills the MAC address of the client in Option 79. The Relay-Forward packet is then forwarded to the DHCPv6 server.

Examples

```
# Enable Option 79 support on the relay agent.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp relay client-link-address enable
```

New feature: mGRE NHS and NHRP packet sending related features

Configuring new features on an NHS

1. Enter system view.
system-view
2. Create an mGRE tunnel interface and enter its view.
interface tunnel *number* mode mgre
3. (Optional.) Specify a DSCP value for outgoing NHRP packets.
nhrp dscp
By default, the DSCP value is 48 for outgoing NHRP packets.
4. (Optional.) Enable the NHS-only feature.
nhrp server-only
By default, the NHS-only feature is disabled.

Configuring new features on an NHC

1. Enter system view.
system-view
2. Create an mGRE tunnel interface and enter its view.
interface tunnel *number* mode mgre
3. (Optional.) Specify a DSCP value for outgoing NHRP packets.
nhrp dscp
By default, the DSCP value is 48 for outgoing NHRP packets.
4. (Optional.) Set the interval at which the NHC sends NHRP registration packets.
nhrp registration time-out *seconds*
By default, an NHC sends NHRP registration packets at intervals of 2400 seconds.
The registration interval must be shorter than the holdtime for NHRP mapping entries.
5. (Optional.) Configure the NHC to include the no-unique flag into outgoing NHRP packets.
nhrp registration no-unique
By default, outgoing NHRP packets do not include the no-unique flag.

Command changes

New command: display nhrp history-map

Use **display nhrp history-map** to display NHRP mapping entries that were cleared or have expired.

Syntax

display nhrp history-map [**count** *count-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

count *count-number*: Displays the specified number of NHRP mapping entries that were cleared or have expired. The value range for the *count-number* argument is 1 to 2000. If you do not specify this option, the command displays all NHRP mapping entries that were cleared or have expired.

Usage guidelines

Use this command to display the following NHRP mapping entries:

- NHRP mapping entries that were cleared by using the **reset nhrp dynamic map** command.
- NHRP mapping entries that have expired because their storage time exceeded the value set by using the **nhrp holdtime** command.

The **display nhrp history-map** command can display a maximum of 2000 entries. A new entry will overwrite the oldest entry for this command when the maximum number is reached.

Examples

Display the most recent two NHRP mapping entries that were cleared or have expired.

```
<Sysname> display nhrp history-map count 2
Number of off-line map: 1984. Alloc memory: 214272
Interface   : Tunnel634
  Destination/mask: 182.134.3.1/32
  Next hop       : 182.134.3.1
  Creation time  : Mon Apr 12 10:23:31 2022
  Delete time   : Mon Apr 12 13:04:28 2022
  Delete reason  : expire
  Hold time     : 7200
  Type          : dynamic
  NBMA address   : 20.1.1.1
Interface   : Tunnel311
  Destination/mask: 182.61.2.1/32
  Next hop       : 182.61.2.1
  Creation time  : Mon Apr 12 10:23:36 2022
  Delete time   : Mon Apr 12 13:04:23 2022
  Delete reason  : expire
  Hold time     : 7200
```

Type : dynamic
NBMA address : 20.1.1.1

Table 56 Command output

Field	Description
Number of off-line map	Number of recorded history NHRP mapping entries that were deleted.
Alloc memory	Amount of memory used by the entries, in bytes.
Interface	Name of an mGRE tunnel interface.
Destination/mask	Protocol address of an NHRP peer NHC.
Next hop	Tunnel address of the NHRP peer NHC.
Creation time	Time when the mapping entry was created.
Delete time	Time when the mapping entry was deleted.
Delete reason	Reason why the mapping entry was deleted: • Expire—The mapping entry holdtime expired. • Tunnel down—Exceptions occurred for the tunnel or public network. • Client purge—The NHC sent purge packets. • Unknown—Other unknown errors.
Hold time	Mapping entry holdtime, in seconds.
Type	Mapping entry type: • static—The entry is statically configured. • cached—The entry is dynamically obtained. • Incomplete—The entry is dynamic and incomplete. • dynamic—The entry is dynamically negotiated.
NBMA address	NBMA network address.

Related commands

display nhrp map

New command: nhrp dscp

Use **nhrp dscp** to specify a DSCP value for the outgoing NHRP packets on an NHS or NHC.

Use **undo nhrp dscp** to restore the default.

Syntax

nhrp dscp *dscp-value*

undo nhrp dscp

Default

The DSCP value is 48.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

In an mGRE scenario, if the DSCP value of NHRP packets is too small when network congestion occurs, the NHRP packets might be dropped. As a result, mGRE tunnel interruption occurs. You can use this command to adjust the DSCP value of NHRP packets to ensure that NHRP packets are preferentially transmitted.

Examples

On tunnel interface Tunnel 1, configure the DSCP value of outgoing NHRP packets as 50.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp dscp 50
```

New command: nhrp registration no-unique

Use **nhrp registration no-unique** to configure an NHC to include the no-unique flag into outgoing NHRP packets.

Use **undo nhrp registration no-unique** to restore the default.

Syntax

nhrp registration no-unique

undo nhrp registration no-unique

Default

An outgoing NHRP packet does not include the no-unique flag on an NHC.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Usage guidelines

When an NHC is registering NHRP information with an NHS, the NHS generates an NHRP mapping entry for the NHC. When the public address of the NHC is changed, the NHC reregisters its latest NHRP information with the NHS. As a result, NHRP mapping entry conflict occurs on the NHS for the NHC. The NHS denies the reregistration of the NHC.

To resolve the issue, use this command on the NHC. With this command, the NHC includes the no-unique flag into NHRP registration and response packets to notify the NHS to overwrite the conflicting NHRP mapping entry with the latest NHC information.

As a best practice to ensure successful NHC reregistration with an NHS in scenarios where the NHCs dynamically obtain addresses, for example, through DHCP, use this command on the NHCs.

Examples

On tunnel interface Tunnel 1, configure mGRE tunnel registration packets to include the no-unique flag.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp registration no-unique
```

New command: nhrp registration time-out

Use **nhrp registration time-out** to set the interval at which an NHC sends NHRP registration packets.

Use **undo nhrp registration time-out** to restore the default.

Syntax

nhrp registration time-out *seconds*

undo nhrp registration time-out

Default

An NHC sends NHRP registration packets at intervals of 2400 seconds.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

seconds: Sets the NHRP registration interval, in seconds. The value range is 1 to 65535.

Usage guidelines

To prevent an NHS from failing to update NHC information in time after the public address of an NHC is modified or the NHRP mapping entry for an NHC on the NHS ages out, use this command on the NHC. To ensure that the NHS can update NHC information in time, make sure the interval at which the NHC sends registration packets is shorter than the holdtime of NHRP mapping entries on the NHS.

Examples

On tunnel interface Tunnel 1, configure the device to send NHRP registration packets at intervals of 300 seconds.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp registration time-out 300
```

Related commands

nhrp holdtime

New command: nhrp server-only

Use **nhrp server-only** to enable the NHS-only feature.

Use **undo nhrp server-only** to disable the NHS-only feature.

Syntax

nhrp server-only

undo nhrp server-only

Default

The NHS-only feature is disabled.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Usage guidelines

When this feature is enabled, the device can act as only an NHS.

When this feature is enabled, the mappings configured by using the **nhrp nhs** command for an NHS cannot take effect. In addition, the device no longer sends registration request packets.

As a best practice, enable this feature only when the device only acts as an NHS.

Examples

On Tunnel interface tunnel 1, enable the NHS-only feature.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp server-only
```

New command: reset nhrp dynamic map

Use **reset nhrp dynamic map** to clear dynamically negotiated NHRP mapping entries.

Syntax

reset nhrp dynamic map [*protocol-address* [*mask*]]

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

protocol-address: Specifies a network layer protocol address in dotted decimal notation.

mask: Specifies the mask of the network layer protocol address, in dotted decimal notation.

Usage guidelines

If you do not specify any parameters, this command clears all dynamic NHRP mapping entries.

To prevent existing dynamic NHRP mapping entries from affecting diagnostic results in debugging operations or in node interaction diagnostic tests, clear the entries before they age out.

Use this command with caution. After this command clears the specified dynamic NHRP mapping entries, the device does not generate these entries until the peer devices register the information again.

To display dynamic NHRP mapping entries that were cleared, use the **display nhrp history-map** command.

Examples

Clear dynamic NHRP mapping entry with IP address 20.20.20.1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] reset nhrp dynamic map 20.20.20.1
```

New command: reset nhrp history-map

Use **reset nhrp history-map** to clear NHRP mapping entries recorded on the device.

Syntax

reset nhrp history-map

Views

User view

Predefined user roles

network-admin

Usage guidelines

Use this command to clear NHRP mapping entries recorded by the **display nhrp history-map** command.

Examples

Clear NHRP mapping entries recorded on the device.

```
<Sysname> reset nhrp history-map
```

Related commands

display nhrp history-map

Modified command: display mgre session

Old syntax

display mgre session [**interface tunnel** *interface-number* [**peer** *ipv4-address*]]
[**verbose**]

New syntax

display mgre session [**count** | [**interface tunnel** *interface-number* [**peer** *ipv4-address*]]
[**dynamic** | **static**]] [**verbose**]]

Views

Any view

Change description

The following keywords were added:

- **count**: Displays mGRE session statistics.
- **dynamic**: Displays detailed information about dynamic mGRE sessions.
- **static**: Displays detailed information about static mGRE sessions.

Modified command: display nhrp map

Old syntax

display nhrp map [**interface tunnel** *interface-number* [**peer** *ipv4-address*]] [**verbose**]

New syntax

display nhrp map [**statistics** | [**interface tunnel** *interface-number* [**peer** *ipv4-address*]]
[**dynamic** | **static**]] [**verbose**]]

Views

Any view

Change description

The following keywords were added:

- **statistics**: Displays statistics about NHRP mapping entries.
- **dynamic**: Displays detailed information about dynamic NHRP mapping entries.
- **static**: Displays detailed information about static NHRP mapping entries.

New feature: Setting the length of called numbers when R2 signaling is used to access the POS terminal

Setting the length of called numbers when R2 signaling is used to access the POS terminal

1. Enter system view.
system-view
2. Enter E1 or T1 interface view.
controller { e1 | t1 } number
3. Create a timeslot set and enable R2 signaling for it.
timeslot-set ts-set-number timeslot-list timeslots-list signal r2
4. Enter R2 CAS view.
cas ts-set-number
5. Set the length of called numbers when R2 signaling is used to access the POS terminal.
posa called-length called-length
The length of called numbers when R2 signaling is used to access the POS terminal is 31 digits.

Command reference

posa called-length

Use **posa called-length** to set the length of called numbers when R2 signaling is used to access the POS terminal.

Use **undo posa called-length** to restore the default.

Syntax

posa called-length *called-length*
undo posa called-length

Default

The length of called numbers when R2 signaling is used to access the POS terminal is 31 digits.

Views

R2 signaling view

Predefined user roles

network-admin

Parameters

called-length: Sets the length of called numbers, in the range of 1 to 31 digits.

Usage guidelines

When the device uses R2 signaling to connect point of sale (POS) terminals, execute this command to meet the real-time requirement of POS terminal services.

Examples

Set the length of called numbers by using R2 signaling to access the POS terminal to 8 digits.

```
<Sysname> system-view
[Sysname] controller e1 2/5/0
[Sysname-e12/5/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e12/5/0] cas 0
[Sysname-cas2/5/0:0] posa called-length 8
```

New feature: Establishing an MQTT connection

Establishing an MQTT connection

About this task

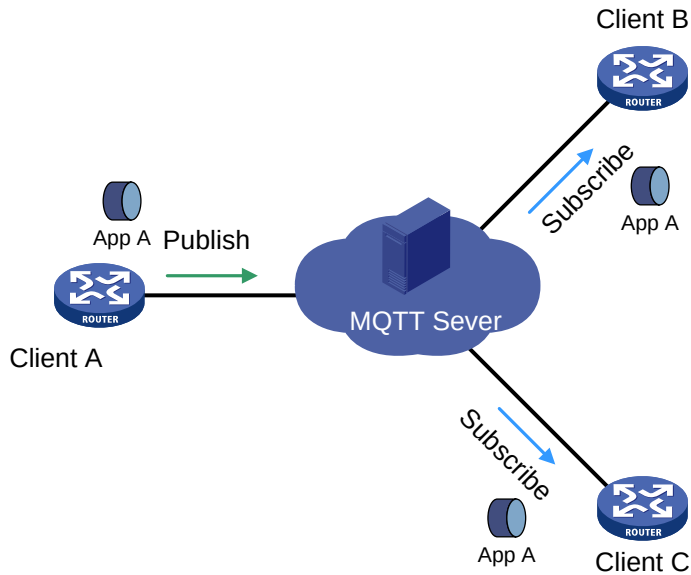
Message Queuing Telemetry Transport (MQTT) is a TCP/IP-based message transfer protocol in client/server model. It can provide real-time and reliable messaging services with lower overhead and bandwidth in remote connection.

As shown in Figure 38, in the MQTT protocol model, the device, acting as an MQTT client, proactively establishes an MQTT connection with the MQTT server. Over the MQTT connection, the device can publish messages to the MQTT server, or subscribe to the MQTT server for messages of other clients. For example, Client A, Client B, and Client C each have established an MQTT connection with the MQTT Server. When Client A publishes information about application A to the MQTT Server, Client B and Client C can subscribe to the MQTT Server for information about application A.

NOTE:

In the current software version, the device supports only establishing an MQTT connection and does not support publishing and subscribing to application messages.

Figure 38 MQTT message publish/subscribe pattern



Restrictions and guidelines

This feature is available only for a device installed with a 5G mobile communication modem.

If you specify an SSL client policy, make sure the policy is correct.

Procedure

1. Enter system view.
system-view
2. Specify an MQTT server.
sim mqtt server { **hostname** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address* }
[**ssl-client-policy** *policy-name*]
By default, no MQTT server is specified.
3. Establish an MQTT connection.
sim mqtt connect [**interval** *interval*] [**retry** *retries*]
By default, the device does not establish an MQTT connection with an MQTT server.
4. Enable keepalive for the MQTT connection.
sim mqtt keepalive [**interval** *interval*] [**retry** *retries*]
By default, keepalive is disabled for the MQTT connection.

Command reference

display sim mqtt statistics

Use **display sim mqtt statistics** to display MQTT connection statistics.

Syntax

display sim mqtt statistics { **all** | **connect** | **connect-fail** | **disconnect** | **packet** }

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

all: Displays all MQTT connection statistics.
connect: Displays statistics about successful MQTT connections.
connect-fail: Displays statistics about failed MQTT connections.
disconnect: Displays statistics about disconnected MQTT connections.
packet: Displays MQTT message statistics.

Usage guidelines

This command is available only for devices installed with a 5G mobile communication modem.

Examples

```
# Display all MQTT connection statistics.
<Sysname> display sim mqtt statistics all
Connection information:
  Sever info: example.com
  Port: 1883
  Connected at: 2022/05/01 10:13:33

  Sever info: example.com
  Port: 8883
  SSL policy name: test-policy
  Connected at: 2022/05/01 01:24:18

Disconnection information:
  Sever info: example.com
  Port: 8883
  SSL policy name: test-policy
  Disconnected at: 2022/05/01 10:13:19
  Disconnection reason: User cleared connection settings.

  Sever info: example.com
  Port: 8883
  SSL policy name: test-policy
  Disconnected at: 2022/05/01 01:24:17
  Disconnection reason: Keepalive timed out.

Connection fail information:
  Connection failed at: 2022/05/01 00:33:21
  Connection fail reason: Refused by the server

  Connection failed at: 2022/05/01 10:23:21
  Connection fail reason: Connection to the server timed out
```

Packet statistics:

Connect	: 4	Connack	: 4
Publish	: 12	Puback	: 1
Pubrec	: 44	Pubrel	: 44
Pubcomp	: 2	Subscribe	: 2
Suback	: 1	Unsubscribe	: 1
Unsuback	: 0	Pingrep	: 0
Pingresp	: 0	SendDisconnect	: 0
RecvDisconnect	: 0	RecvData	: 0
SendData	: 20		

Table 57 Command output

Field	Description
Connection information	Successful MQTT connection information.
Sever info	Domain name or IP address of the MQTT server.
Port	Server-end port number for MQTT connection.
SSL policy-name	SSL client policy used for establishing an encrypted MQTT connection.
Connected at	Time at which the device established a connection to the MQTT server.
Disconnection information	MQTT disconnection information.
Disconnected at	Time at which the device was disconnected from the MQTT server.
Disconnection reason	Reason that caused disconnection of the device from the MQTT server. • Keepalive timed out. • User cleared connection settings. • Server sent disconnect packet. • Memory usage alert.
Connection fail information	Failed MQTT connection information.
Connection failed at	Time at which the device failed to establish a connection with the MQTT server.
Connection fail reason	Reason that caused failure of the device to establish a connection with the MQTT server. • Refused by the server. • Connection to the server timed out. • Server sent disconnect packet. • Memory usage alert.
Packet statistics	Statistics of messages for MQTT connection.
Connect	Number of connection requests sent by the device to the MQTT server.
Connack	Number of connection-request responses that the device received from the MQTT server.
Publish	Number of information publishings from the device to the MQTT server.
Puback	Number of information-publishing responses that the device received from the MQTT server.
Pubrec	Number of recorded information publishings from the device to the MQTT server.
Pubrel	Number of released information publishings from the device to the MQTT server.

Field	Description
Pubcomp	Number of completed information publishings from the device to the MQTT server.
Subscribe	Number of subscriptions from the device to the MQTT server.
Suback	Number of subscription acknowledgements from the MQTT server.
Unsubscribe	Number of canceled subscriptions from the device to the MQTT server.
Unsuback	Number of subscription cancel acknowledgement from the MQTT server.
Pingreq	Number of keepalive messages sent from the device to the MQTT server.
Pingresp	Number of keepalive acknowledge messages that the device received from the MQTT server.
SendDisconnect	Number of disconnection requests that the device sent to the MQTT server.
RecvDisconnect	Number of disconnection requests that the device received from the MQTT server.
RecvData	Number of data packets that the device received from the MQTT server.
SendData	Number of data packets that the device sent to the MQTT server.

Related commands

reset sim mqtt statistics

display sim mqtt status

Use **display sim mqtt status** to display the MQTT connection status.

Syntax

display sim mqtt status

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command is available only for devices installed with a 5G mobile communication modem.

Examples

Display MQTT connection status.

```
<Sysname> display sim mqtt status
Connection status      : Established
Reconnection interval  : 10s
Reconnection retries   : 5
Keepalive status       : Normal
Keepalive interval     : 30s
Keepalive retries      : 5
```

Table 58 Command output

Field	Description
Connection status	Connection status between the device and MQTT server. • Idle—No connection is established. • Established—A connection has been established.
Connection interval	Intervals at which the device retries connection to the MQTT server, in seconds.
Connection retries	Maximum number of connection retries from the device to the MQTT server.
Keepalive status	Keepalive status between the device and MQTT server: • Abnormal: The connection is not alive. • Normal: The connection is alive. • -: Keepalive is not enabled.
Keepalive interval	Intervals at which the device sends keepalive messages to the MQTT server, in seconds.
Keepalive retries	Maximum number of keepalive message transmission retries.

Related commands

sim mqtt connect

sim mqtt keepalive

reset sim mqtt statistics

Use **reset sim mqtt statistics** to clear MQTT connection statistics.

Syntax

reset sim mqtt statistics { all | connect | connect-fail | disconnect | packet }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all MQTT connection statistics.

connect: Clears successful MQTT connection statistics.

connect-fail: Clears failed MQTT connection statistics.

disconnect: Clears disconnected MQTT connection statistics.

packet: Clears MQTT message statistics.

Usage guidelines

This command is available only for devices installed with a 5G mobile communication modem.

Examples

Clear all MQTT connection statistics.

```
<Sysname> reset sim mqtt statistics all
```

Related commands

display sim mqtt statistics

sim mqtt connect

Use **sim mqtt connect** to establish an MQTT connection.

Use **undo sim mqtt connect** to disconnect the MQTT connection.

Syntax

sim mqtt connect [**interval** *interval*] [**retry** *retries*]

undo sim mqtt connect

Default

The device does not establish an MQTT connection with an MQTT server.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval at which the device retries connection to the MQTT server. The value is in the range of 0 to 3600, in seconds. The default value is 60 seconds.

retry *retries*: Specifies the maximum number of connection retries. The value is in the range of 1 to 255. The default value is 3.

Usage guidelines

After this command is configured, the device, acting as an MQTT client, will immediately attempt to establish an MQTT connection to the MQTT server. If the device fails to establish the connection, it will create an MQTT reconnection counter to count the reconnection attempts of the device to the MQTT server.

- If the device establishes a connection to the MQTT server successfully before the maximum number of connection retries is reached, the device will clear the reconnection count recorded on the device.
- If the device fails to establish a connection to the MQTT server when the maximum number of connection retries is reached, the connection establishment fails and the device will no longer attempt a reconnection. Check the settings of the MQTT server, including the IP address and domain name and then use this command to establish a connection again.

This command is available only for devices installed with a 5G mobile communication modem.

Examples

Enable the device to establish an MQTT connection and to retry connection to the MQTT server at intervals of 5 seconds after the connection fails. Set the maximum number of connection retries to 10.

```
<Sysname> system-view
```

```
[Sysname] sim mqtt connect interval 5 retry 10
```

sim mqtt keepalive

Use **sim mqtt keepalive** to enable keepalive for the MQTT connection.

Use **undo sim mqtt keepalive** to disable keepalive for the MQTT connection.

Syntax

```
sim mqtt keepalive [ interval interval ] [ retry retries ]  
undo sim mqtt keepalive
```

Default

Keepalive is disabled for the MQTT connection.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval at which keepalive messages are sent. The value range for the argument is 1 to 65535, in seconds. The default value is 180 seconds.

retry *retries*: Specifies the maximum number of keepalive message transmission retries. The value range for the argument is 1 to 255. The default value is 3.

Usage guidelines

For information exchange between the MQTT client and MQTT server at any time, you can configure this command after the MQTT connection is established for the MQTT client and MQTT server to maintain the MQTT connection by exchanging keepalive messages.

The MQTT client sends a keepalive message to the MQTT server at the specified interval, and the MQTT server replies a response after receiving the keepalive message. If the device does not receive a response message from the MQTT server, it will create an MQTT connection keepalive counter to count the keepalive messages resent to the MQTT server.

- If the device receives a response message from the MQTT server before the maximum number of keepalive transmission retries is reached, the device will delete the keepalive counter.
- If the device does not receive a response message from the MQTT server when the maximum number of keepalive transmission retries is reached, the connection with the MQTT server is disconnected and the device will no longer send keepalive messages to the MQTT server and will disconnect from the MQTT server. After the MQTT connection is disconnected, reconfigure the **sim mqtt connect** command to try to re-establish a connection with the MQTT server.

This command is available only for devices installed with a 5G mobile communication modem.

Usage guidelines

Set the interval at which the device sends a keepalive message to the MQTT server to 30 seconds and the maximum keepalive transmission retries to 5.

```
<Sysname> system-view
```

```
[Sysname] sim mqtt keepalive interval 30 retry 5
```

sim mqtt server

Use **sim mqtt server** to specify an MQTT server.

Use **undo sim mqtt server** to restore the default.

Syntax

```
sim mqtt server { hostname name | ip ipv4-address | ipv6 ipv6-address }  
[ ssl-client-policy policy-name ]  
undo sim mqtt server
```

Default

No MQTT server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

hostname *name*: Specifies an MQTT server by its host name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, hyphens (-), underscores (_), and dots (.).

ip *ipv4-address*: Specifies an MQTT server by its IPv4 address, in dotted decimal notation.

ipv6 *ipv6-address*: Specifies an MQTT server by its IPv6 address

ssl-client-policy *policy-name*: Specifies the SSL client policy that the device uses to establish an MQTT connection with the MQTT server. The argument is a case-insensitive string of 1 to 31 characters. If you do not specify this option, the MQTT client establishes a non-encrypted connection with the MQTT server.

Usage guidelines

This command is available only for devices installed with a 5G mobile communication modem.

The MQTT client and MQTT server can establish an unencrypted MQTT connection or an SSL-based encrypted MQTT connection.

- The server-end port number used for the unencrypted connection is 1883. By default, unencrypted MQTT connection is established.
- The server-end port number used for the encrypted connection is 8883. When establishing an encrypted MQTT connection, the device will act as an SSL client. You must configure the SSL client security policy matching the SSL server (MQTT server). For more information about SSL client policies, see SSL in the *Security Configuration Guide*.

Execute the **undo sim mqtt server** command with caution. It will disconnect the established MQTT connection.

Examples

Specify the MQTT server with domain name example.com.

```
<Sysname> system-view
```

```
[Sysname] sim mqtt server hostname example.com
```

New feature: Configuring packet duplication optimization parameters

Configuring packet duplication optimization parameters

About this task

When packet duplication optimization is enabled on the device, the sender replicates the packets to be sent and selects an additional path reachable to the destination as the forwarding path for the

packets. After receiving the packets, the receiver reorders the packets to ensure the integrity and continuity of the packets.

The sender can select a path by using the packet duplication algorithm, by using the RIR feature, or by using a static path, with different priorities.

- If packet duplication RIR is enabled, the device selects a path based on the link priority, link quality, and link bandwidth. This method has the highest priority.
- If a path is manually specified on the device and no path calculated by using the packet duplication RIR algorithm exists, the device uses the manually specified path. A manually specified path has higher priority than the path selected by using the packet duplication algorithm.
- If the device detects that neither a path selected by using the packet duplication RIR feature nor a manually specified path exists, it selects the first path in the routing table that has the same cost as the original path by using the packet duplication algorithm.

With the packet reorder feature, the sender numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n, and then replicates and forwards the packets. The receiver discards the packets with the same sequence number and reorders them before forwarding them. If no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Restrictions and guidelines

Packet duplication RIR takes effect only if RIR is enabled on the device. For more information about RIR, see RIR configuration in *Layer 3—IP Routing Configuration Guide*.

Make sure an SDWAN tunnel exists for a manually specified packet duplication path. If the same SDWAN tunnel is configured as the packet duplication path multiple times, the most recent configuration takes effect. If multiple paths are specified for the same destination, only one path will be selected as the packet duplication path by using a specific algorithm. Manually specifying a packet duplication path is available only in an SDWAN network.

Enabling packet duplication RIR

1. Enter system view.
system-view
2. Create a WAAS policy and enter WAAS policy view.
waas policy *policy-name*
3. Specify a class and enter WAAS policy class view.
class *class-name* [**insert-before** *existing_class*]
4. Enable packet duplication RIR.
packet-dup rir enable
By default, packet duplication RIR is disabled.

Manually specifying a packet duplication path in an SDWAN network

1. Enter system view.
system-view
2. Manually specify a packet duplication path in an SDWAN network.

```

waas packet-dup sdwan static-path { destination-ip dest-ipv4-address
{ dest-mask-length | dest-mask } | destination-ipv6 dest-ipv6-address
dest-prefix-length } [ vpn-instance vpn-instance-name ] interface interface-type
interface-number peer-site-id peer-site-id peer-device-id peer-device-id
peer-interface-id peer-interface-id [ priority priority ]

```

By default, no packet duplication path is manually specified in an SDWAN network.

Setting the packet duplication reorder timeout timer

1. Enter system view.
system-view
 2. Create a WAAS policy and enter WAAS policy view.
waas policy *policy-name*
 3. Specify a class and enter WAAS policy class view.
class *class-name* [**insert-before** *existing_class*]
 4. Set the packet duplication reorder timeout timer.
packet-dup reorder timeout *timeout*
- By default, the packet duplication reorder timeout timer is 100 ms.

Command reference

packet-dup reorder timeout

Use **packet-dup reorder timeout** to set the packet duplication reorder timeout timer.

Use **undo packet-dup reorder timeout** to restore the default.

Syntax

packet-dup reorder timeout *timeout*

undo packet-dup reorder timeout

Default

The packet duplication reorder timeout timer is 100 ms.

Views

WAAS policy class view

Predefined user roles

network-admin

Parameters

timeout: Specifies the packet duplication reorder timeout timer, in the range of 1 to 65535 milliseconds.

Usage guidelines

With the packet reorder feature, the sender numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n, and then replicates and forwards the packets. The receiver discards the packets with the same sequence number and reorders them before forwarding them. If no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number

arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Examples

```
# Set the packet duplication reorder timeout timer to 100 milliseconds for WAAS class AFS.
```

```
<Sysname> system-view
[Sysname] waas policy waas_global
[Sysname-waaspolicy-waas_global] class AFS
[Sysname-waaspolicy-waas_global-AFS] packet-dup reorder timeout 100
```

packet-dup rir enable

Use **packet-dup rir enable** to enable packet duplication RIR.

Use **undo packet-dup rir enable** to disable packet duplication RIR.

Syntax

packet-dup rir enable

undo packet-dup rir enable

Default

Packet duplication RIR is disabled.

Views

WAAS policy class view

Predefined user roles

network-admin

Usage guidelines

With packet duplication RIR enabled, the device selects a path based on the link priority, link quality, and link bandwidth.

Packet duplication RIR takes effect only if RIR is enabled on the device. For more information about RIR, see RIR configuration in *Layer 3—IP Routing Configuration Guide*.

The sender can select a path by using the packet duplication RIR feature or by using a static path.

- If a path is manually specified on the device and a path calculated by using the packet duplication RIR algorithm exists, the device uses the path selected by using the packet duplication RIR algorithm.
- If the device detects that neither a path selected by using the packet duplication RIR feature nor a manually specified path exists, it selects the first path in the routing table that has the same cost as the original path by using the packet duplication algorithm.

Examples

```
# Enable packet duplication RIR for WAAS policy class AFS.
```

```
<Sysname> system-view
[Sysname] waas policy waas_global
[Sysname-waaspolicy-waas_global] class AFS
[Sysname-waaspolicy-waas_global-AFS] packet-dup rir enable
```

Related commands

optimize

rir sdwan (*Layer 3—IP Routing Command Reference*)

waas packet-dup sdwan static-path

Use **waas packet-dup sdwan static-path** to manually specify a packet duplication path in an SDWAN network.

Use **undo waas packet-dup sdwan static-path** to remove a packet duplication path in an SDWAN network.

Syntax

```
waas packet-dup sdwan static-path { destination-ip dest-ipv4-address { dest-mask-length | dest-mask } | destination-ipv6 dest-ipv6-address dest-prefix-length } [ vpn-instance vpn-instance-name ] interface interface-type interface-number peer-site-id peer-site-id peer-device-id peer-device-id peer-interface-id peer-interface-id [ priority priority ]
```

```
undo waas packet-dup sdwan static-path [ { destination-ip dest-ipv4-address { dest-mask-length | dest-mask } | destination-ipv6 dest-ipv6-address dest-prefix-length } [ vpn-instance vpn-instance-name ] [ interface interface-type interface-number ] [ peer-site-id peer-site-id peer-device-id peer-device-id peer-interface-id peer-interface-id ] [ priority priority ] ]
```

Default

No packet duplication path exists in an SDWAN network.

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip *dest-ip-address*: Specifies a destination IPv4 address in dotted decimal notation.

dest-mask-length: Specifies a mask length for the destination IPv4 address, in the range of 0 to 32.

dest-mask: Specifies a subnet mask for the destination IPv4 address, in dotted decimal notation.

destination-ipv6 *dest-ipv6-address*: Specifies a destination IPv6 address.

dest-prefix-length: Specifies a prefix length for the destination IPv6 address, in the range of 1 to 128.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

interface *interface-type* *interface-number*: Specifies an interface by its type and number. Only tunnel interfaces are supported.

peer-site-id *peer-site-id*: Specifies a site ID in the range of 1 to 65535.

peer-device-id *peer-device-id*: Specifies a device ID in the range of 1 to 255.

peer-interface-id *peer-interface-id*: Specifies an interface ID in the range of 1 to 255.

priority *priority*: Specifies a priority for the static path, in the range of 1 to 255. The default priority is 60. A larger value indicates a higher priority.

Usage guidelines

Make sure the specified SDWAN tunnel already exists. To view the SDWAN tunnels on the device, execute the **display sdwan tte connection** command.

If the same SDWAN tunnel is configured as the packet duplication path multiple times, the most recent configuration takes effect. If multiple paths are specified for the same destination, only one path will be selected as the packet duplication path by using a specific algorithm.

The sender can select a path by using the packet duplication RIR feature or by using a static path.

- If a path is manually specified on the device and a path calculated by using the packet duplication RIR algorithm exists, the device uses the path selected by using the packet duplication RIR algorithm.
- If the device detects that neither a path selected by using the packet duplication RIR feature nor a manually specified path exists, it selects the first path in the routing table that has the same cost as the original path by using the packet duplication algorithm.

If you do not specify any keywords when executing the **undo waas packet-dup sdwan static-path** command, the command deletes all manually specified packet duplication paths.

This command is available only in an SDWAN network.

Examples

Manually specify a packet duplication path in an SDWAN network.

```
<Sysname> system-view
```

```
[Sysname] waas packet-dup sdwan static-path ip 200.1.1.0 24 vpn-instance vpn-1 local tunnel  
1 peer site-id 2 device-id 3 interface-id 5 priority 50
```

Related commands

display sdwan tte connection (*SDWAN Command Reference*)

New feature: Setting the reorder timeout timer for load balancing packets

Setting the reorder timeout timer for load balancing packets

About this task

With load balancing enabled on the device, the sender forwards the packets on all paths with the same cost to the destination. This can cause packet disorder on the receiver. WAAS numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n. The receiver reorders and forwards the packets. With the load balancing packet reorder timeout timer set, if no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Restrictions and guidelines

This feature is supported only for per-packet load balancing.

Procedure

1. Enter system view.
system-view
2. Set the reorder timeout timer for load balancing packets.
waas load-balance reorder timeout *timeout*

By default, the reorder timeout timer is 100 ms for load balancing packets.

Command reference

display waas statistics load-balance

Use **display waas statistics load-balance** to display load sharing packet statistics information.

Syntax

display waas statistics load-balance { ipv4 | ipv6 }

Views

Any view

Predefined user roles

- network-admin
- network-operator

Parameters

- ipv4**: Displays IPv4 packet statistics.
- ipv6**: Displays IPv6 packet statistics.

Usage guidelines

This command is supported only for packets load shared in per-packet mode.

Examples

```
# Display IPv4 load sharing packet statistics.
<Sysname> display waas statistics load-balance ipv4
Packet Order Preservation:
  In-order packets sent                               :200
  Out-of-order packets sent                           :19
  Out-of-order packets cached                         :40
  Cached packets sent in order                       :40
  Cache failed packets sent                           :0
  Cached packets sent on timeout                      :0
  Out-of-order fragmented packets sent                :1
  Out-of-order fragmented packets cached              :3
  Cached fragmented packets sent in order              :3
  Cached fragmented packets sent on timeout            :3
```

Table 59 Command output

Field	Description
Packet Order Preservation	Packet statistics for packet order preservation on the receiver.
In-order packets sent	Number of in-order packets sent.
Out-of-order packets sent	Number of out-of-order packets sent.
Out-of-order packets cached	Number of out-of-order packets cached.
Cached packets sent in order	Number of cached packets sent in order.
Cache failed packets sent	Number of packets sent after failed to be cached.
Cached packets sent on timeout	Number of cached packets sent out of order after

	timeout.
Out-of-order fragmented packets sent	Number of out-of-order fragmented packets sent.
Out-of-order fragmented packets cached	Number of out-of-order fragmented packets cached.
Cached fragmented packets sent in order	Number of cached fragmented packets sent in order.
Cached fragmented packets sent on timeout	Number of cached fragmented packets sent out of order after timeout.

reset waas statistics load-balance

Use **reset waas statistics load-balance** to clear load balancing packet statistics.

Syntax

reset waas statistics load-balance { **ipv4** | **ipv6** }

Views

User view

Predefined user roles

network-admin

Parameters

ipv4: Clears IPv4 packet statistics.

ipv6: Clears IPv6 packet statistics.

Usage guidelines

This command is supported only for packets load shared in per-packet mode.

Examples

Clears IPv4 load sharing packet statistics.

```
<Sysname> reset waas statistics load-balance ipv4
```

Related commands

display waas statistics load-balance

waas load-balance reorder timeout

Use **waas load-balance reorder timeout** to set the reorder timeout timer for load balancing packets.

Use **undo waas load-balance reorder timeout** to restore the default.

Syntax

waas load-balance reorder timeout *timeout*

undo waas load-balance reorder timeout

Default

The reorder timeout timer is 100 ms for load balancing packets.

Views

System view

Predefined user roles

network-admin

Parameters

timeout: Specifies the reorder timeout timer for load balancing packets, in the range of 1 to 65535 milliseconds.

Usage guidelines

With load balancing enabled on the device, the sender forwards the packets on all paths with the same cost to the destination. This can cause packet disorder on the receiver. WAAS numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n. The receiver reorders and forwards the packets. With the load balancing packet reorder timeout timer set, if no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Examples

Set the reorder timeout timer for load balancing packets.

```
<Sysname> system-view
```

```
[Sysname] waas load-balance reorder timeout 100
```

New feature: Configuring TCP MSS automatic adjustment

Configuring TCP MSS automatic adjustment

About this task

In environments such as GRE, SSL VPN, or IPsec VPN, the device must add new headers to TCP packets for VPN services. If the size of these new TCP packets exceeds the negotiated TCP MSS, multiple intermediate devices might fragment these packets, resulting in low forwarding efficiency. An appropriate TCP MSS is essential for data transmission. However, manual TCP MSS configuration for all VPN services is an effort, because the APPENDLEN value varies by VPN service type.

To resolve this issue, enable automatic TCP MSS adjustment on VPN intermediate devices. With this feature enabled, the device can automatically adjust the TCP MSS according to the VPN service type, ensuring that TCP segments are not re-fragmented along the path to the destination.

After you enable automatic TCP MSS adjustment, the minimum value of the following MSSs takes effect during TCP connection establishment:

- The MSS value carried by the TCP packets.
- The MSS value calculated based on the VPN service type and the IPv4 MTU. The calculation formula is as follows:
$$MSS = \text{interface MTU} - \text{IP header length} - \text{TCP header length} - \text{APPENDLEN}$$
- APPENDLEN represents the total length of fields added to a TCP packet for VPN services.
- To set the IPv4 MTU of an interface, use the **ip mtu** command.
- The interface MSS set by the **tcp mss** command.
- The global MSS set by the **tcp auto-adjust-mss** command.

After you disable automatic TCP MSS adjustment, the minimum value of the following MSSs takes effect during TCP connection establishment:

- The MSS value carried by the TCP packets.
- The interface MSS set by the **tcp mss** command.

Hardware and feature compatibility

Hardware	Feature compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	Yes
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	Yes
MSR 2630	Yes
MSR3600-28, MSR3600-51	Yes
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	Yes
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	Yes
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	Yes
MSR3610-G, MSR3620-G	Yes
MSR3640-X1-HI	Yes

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	Yes

Hardware	Feature compatibility
MSR2600-10-X1-WiNet	Yes
MSR2630-WiNet	Yes
MSR3600-28-WiNet	Yes
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	Feature compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	Yes
MSR3600-28-XS	Yes
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	Yes
MSR3610-IE-XS	Yes
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Feature compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	No

Restrictions and guidelines

Enabling automatic TCP MSS adjustment has an impact on session establishment and forwarding performance, because the device needs to make an additional TCP MSS decision during packet forwarding. To ensure high forwarding performance, you can disable this feature.

This feature takes effect only on TCP connections that are established after the configuration and not on the TCP connections that already exist.

Procedure

1. Enter system view.

system-view

2. Enable TCP MSS automatic adjustment.

tcp auto-adjust-mss enable

By default, TCP MSS automatic adjustment is disabled.

3. (Optional.) Set the global TCP MSS.

tcp auto-adjust-mss value

By default, the global TCP MSS is 1460 bytes.

Command reference

tcp auto-adjust-mss

Use **tcp auto-adjust-mss** to set the global TCP maximum segment size (MSS).

Use **undo tcp auto-adjust-mss** to restore the default.

Syntax

tcp auto-adjust-mss *value*

undo tcp auto-adjust-mss

Default

The global TCP MSS is 1460 bytes.

Views

System view

Predefined user roles

network-admin

Parameters

value: Sets the global TCP MSS, in bytes. The value range for this argument is 128 to 63960. The default value is 1460.

Usage guidelines

Application scenarios

Automatic TCP MSS adjustment is applicable to GRE, SSL VPN, and IPsec VPN environments. With this feature enabled, the device can automatically adjust the TCP MSS according to the VPN service type, ensuring that TCP segments are not re-fragmented along the path to the destination.

Operating mechanism

After you enable automatic TCP MSS adjustment, the minimum value of the following MSSs takes effect during TCP connection establishment:

- The MSS value carried by the TCP packets.
- The MSS value calculated based on the VPN service type and the IPv4 MTU. The calculation formula is as follows:

$$\text{MSS} = \text{interface MTU} - \text{IP header length} - \text{TCP header length} - \text{APPENDLEN}$$

- APPENDLEN represents the total length of fields added to a TCP packet for VPN services.
- To set the IPv4 MTU of an interface, use the **ip mtu** command.
- The interface MSS set by the **tcp mss** command.

- The global MSS set by the **tcp auto-adjust-mss** command.

Restrictions and guidelines

The global TCP MSS takes effect only after automatic TCP MSS adjustment is enabled.

The global TCP MSS takes effect only on TCP connections that are established after it is configured. It does not take effect on TCP connections that have been established before it is configured.

Examples

```
# Set the global TCP MSS to 1450 bytes.
<Sysname> system-view
[Sysname] tcp auto-adjust-mss 1450
```

Related commands

ip mtu

tcp auto-adjust-mss enable

tcp mss

tcp auto-adjust-mss enable

Use **tcp auto-adjust-mss enable** to enable automatic TCP MSS adjustment.

Use **undo tcp auto-adjust-mss enable** to disable automatic TCP MSS adjustment.

Syntax

tcp auto-adjust-mss enable

undo tcp auto-adjust-mss enable

Default

Automatic TCP MSS adjustment is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Application scenarios

In environments such as GRE, SSL VPN, or IPsec VPN, the device must add new headers to TCP packets for VPN services. If the size of these new TCP packets exceeds the negotiated TCP MSS, multiple intermediate devices might fragment these packets, resulting in low forwarding efficiency. An appropriate TCP MSS is essential for data transmission. However, manual TCP MSS configuration for all VPN services is an effort, because the APPENDLEN value varies by VPN service type.

To resolve this issue, enable automatic TCP MSS adjustment on VPN intermediate devices. With this feature enabled, the device can automatically adjust the TCP MSS according to the VPN service type, ensuring that TCP segments are not re-fragmented along the path to the destination.

Operating mechanism

After you enable automatic TCP MSS adjustment, the minimum value of the following MSSs takes effect during TCP connection establishment:

- The MSS value carried by the TCP packets.
 - The MSS value calculated based on the VPN service type and the IPv4 MTU.
 - The interface MSS set by the **tcp mss** command.
 - The global MSS set by the **tcp auto-adjust-mss** command.
- After you disable automatic TCP MSS adjustment, the minimum value of the following MSSs takes effect during TCP connection establishment:
- The MSS value carried by the TCP packets.
 - The interface MSS set by the **tcp mss** command.

Restrictions and guidelines

When you configure the automatic TCP MSS adjustment feature, follow these guidelines:

- Enabling automatic TCP MSS adjustment has an impact on session establishment and forwarding performance, because the device needs to make an additional TCP MSS decision during packet forwarding. To ensure high forwarding performance, you can disable this feature.
- The automatic TCP MSS adjustment feature takes effect only on TCP connections that are established after it is configured. It does not take effect on TCP connections that have been established before it is configured.

Examples

```
# Enable automatic TCP MSS adjustment.
<Sysname> system-view
[Sysname] tcp auto-adjust-mss enable
```

Related commands

```
ip mtu
tcp auto-adjust-mss
tcp mss
```

New feature: Configuring BGP GR

Configuring BGP GR

About this task

When the TCP connection goes down, the hold timer expires, or the address families supporting route exchange change, BGP tears down and then re-establishes the peer sessions, which will cause traffic interruption. To avoid traffic interruption in these cases, configure this feature to enable BGP to reset peer sessions gracefully.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. (Optional.) Set the extra time to wait after the restart timer expires.
peer { group-name | ipv4-address [mask-length] | ipv6-address [prefix-length] } graceful-restart timer restart extra { time | no-limit }

By default, the extra time to wait after the restart timer expires is 0 seconds.

4. (Optional.) Enable BGP to reset peer sessions gracefully.

graceful-restart peer-reset [all]

By default, BGP does not reset peer sessions gracefully.

Command reference

graceful-restart peer-reset

Use **graceful-restart peer-reset** to enable BGP to reset peer sessions gracefully.

Use **undo graceful-restart peer-reset** to disable BGP from resetting peer sessions gracefully.

Syntax

graceful-restart peer-reset [all]

undo graceful-restart peer-reset

Default

BGP does not reset peer sessions gracefully.

Views

BGP instance view

Predefined user roles

network-admin

Parameters

all: Enables BGP to reset peer sessions gracefully when the TCP connection goes down, the hold timer expires, or the address families supporting route exchange change. If you do not specify this keyword, BGP resets peer sessions gracefully only when the address families supporting route exchange change.

Usage guidelines

When the TCP connection goes down, the hold timer expires, or the address families supporting route exchange change, BGP tears down and then re-establishes the peer sessions, which will cause traffic interruption. To avoid traffic interruption in these cases, execute this command to enable BGP to reset peer sessions gracefully.

Examples

```
# Enable BGP to reset peer sessions gracefully.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] graceful-restart
```

```
[Sysname-bgp-default] graceful-restart peer-reset
```

Related commands

graceful-restart

peer graceful-restart timer restart extra

Use **peer graceful-restart timer restart extra** to set the extra time to wait after the restart timer expires.

Use **undo peer graceful-restart timer restart extra** to restore the default.

Syntax

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
graceful-restart timer restart extra { time | no-limit }  
  
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
graceful-restart timer restart extra
```

Default

The extra time to wait after the restart timer expires is 0 seconds.

Views

BGP instance view

BGP-VPN instance view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command specifies all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command specifies all dynamic peers in the subnet.

time: Specifies the extra time to wait after the restart timer expires, in the range of 0 to 86400 seconds.

no-limit: Sets an unlimited time to wait for BGP session re-establishment.

Usage guidelines

After the active/standby switchover or BGP restart completes, the GR helper marks the routes it learned from the GR restarter as stale routes. If the GR helper fails to establish a BGP session after both the GR timer and the extra timer to wait expire, the GR helper removes the stale routes.

If you specify the **no-limit** keyword, the GR helper does not start the End-Of-RIB marker wait timer after BGP peer session re-establishment. Instead, it keeps waiting for the End-Of-RIB marker sent from the peer.

Examples

```
# Set the extra time to wait after the restart timer expires to 100 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] peer 10.1.100.2 graceful-restart timer restart extra 100
```

Related commands

graceful-restart timer restart

New feature: Support for filtering routes by the Priority-Color extended community attribute

Configuring a Priority-Color extended community list

1. Enter system view.
system-view
2. Configure a Priority-Color extended community list.
ip extcommunity-list *ext-comm-list-number* [**index** *index-number*] { **deny** | **permit** } **priority-color** { **basic** *priority-color*<1-32> [**not-match-priority**] | **advanced** *regular-expression* }

Command reference

display ip extcommunity-list

Use **display ip extcommunity-list** to display BGP extended community list information.

Syntax

display ip extcommunity-list [*ext-comm-list-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

ext-comm-list-number: Specifies an extended community list by its number in the range of 1 to 65535. If you do not specify this argument, the command displays information about all BGP extended community lists.

Examples

Display information about BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
```

Extended Community List Number 1

```
      Index: 1           Mode:Permit RT: 3:1 SoO: 3:2
      Index: 2           Mode:Permit RT: 3:1 SoO: 3:2 SoO: 5:2
      Index: 3           Mode:Permit RT: 3:1 SoO: 3:2 RT: 6:7
```

Table 60 Command output

Field	Description
Extended Community List Number	Extended community list.

Field	Description
Index	Index of the extended community list entry.
Mode	Match mode: • Permit. • Deny.
rt	Route Target (RT) extended community attribute.
soo	Site of Origin (SoO) extended community attribute.

ip extcommunity-list

Use **ip extcommunity-list** to configure an extended community list.

Use **undo ip extcommunity-list** to remove an extended community list.

Syntax

```
ip extcommunity-list ext-comm-list-number [ index index-number ] { deny | permit }
priority-color { basic priority-color&<1-32> [ not-match-priority ] | advanced
regular-expression }

undo ip extcommunity-list ext-comm-list-number [ index index-number | { deny | permit }
[ priority-color { basic priority-color&<1-32> | advanced regular-expression } ] ]
```

Default

No extended community lists exist.

Views

System view

Predefined user roles

network-admin

Parameters

ext-comm-list-number: Specifies an extended community list number in the range of 1 to 65535.

index index-number: Specifies an index for the extended community list entry, in the range of 1 to 4294967295. An extended community list entry with a smaller index number is matched first. If you do not specify this option, the index number starts from 1 and increases by 1 for each of the consecutive extended community list entries.

deny: Specifies the match mode for the extended community list as **deny**.

permit: Specifies the match mode for the extended community list as **permit**.

priority-color: Filters routes by the Priority-Color extended community attribute.

basic priority-color&<1-32>: Specifies a list of Priority-Color extended community attributes. &<1-32> indicates that you can specify a maximum of 32 Priority-Color extended community attributes. The value for the *priority-color* argument is a string of 3 to 12 characters in *Priority:Site ID:Device ID* or *Priority:Site ID* format:

- The priority value range is 0 to 15.
- The site ID range is 1 to 65535.
- The device ID range is 1 to 255. If you do not specify the device ID of a Priority-Color extended community attribute, all Priority-Color extended community attributes with the same site ID as that Priority-Color extended community attribute will be matched.

not-match-priority: Ignores the Priority field of Priority-Color extended community attributes. If you specify this keyword, the specified extended community list matches against only the Site ID and Device ID fields of Priority-Color extended community attributes. If you do not specify this keyword, a route can match the specified extended community list only when its Priority-Color extended community attribute exactly matches the specified extended community list.

advanced *regular-expression*: Specifies a regular expression to filter Priority-Color extended community attributes. The value for the *regular-expression* argument is a string of 1 to 63 characters. If the Priority-Color extended community attribute of a route matches the specified regular expression, the route can match the specified extended community list.

Usage guidelines

If you execute this command multiple times for an extended community list entry, the most recent configuration takes effect.

Examples

Configure extended community list 3 to permit routes with Priority-Color 10:10:10 to pass.

```
<Sysname> system-view
```

```
[Sysname] ip extcommunity-list 3 permit priority-color 10:10:10
```

Related commands

apply extcommunity

apply extcommunity priority-color

display ip extcommunity-list

if-match extcommunity

Configuring the Priority-Color extended community attribute for BGP routes

1. Enter system view.
system-view
2. Enter routing policy node view.
route-policy *route-policy-name* { deny | permit } node *node-number*
3. Set the Priority-Color extended community attribute for BGP routes.
apply extcommunity priority-color *priority-color*&<1-32> [additive]

Command reference

apply extcommunity priority-color

Use **apply extcommunity priority-color** to set the Priority-Color extended community attribute for BGP routes.

Use **undo apply extcommunity priority-color** to remove the specified Priority-Color extended community attribute for BGP routes.

Syntax

apply extcommunity priority-color *priority-color*&<1-32> [additive]

undo apply extcommunity priority-color *priority-color*&<1-32>

Default

No Priority-Color extended community attribute is set for BGP routes.

Views

Routing policy node view

Predefined user roles

network-admin

Parameters

priority-color<1-32>: Sets the Priority-Color extended community attribute, a string of 3 to 12 characters. <1-32> indicates that you can specify a maximum of 32 Priority-Color extended community attributes. The value for the *priority-color* argument is in *Priority:Site ID:Device ID* or *Priority:Site ID* format:

- The priority value range is 0 to 15. A smaller priority value indicates a higher priority.
- The site ID range is 1 to 65535 and the device ID range is 1 to 255. You can specify an SDWAN device on the SDWAN network by its site ID and device ID.

additive: Adds the specified Priority-Color extended community attribute to the original Priority-Color extended community attribute of BGP routes. If you do not specify this keyword, the specified Priority-Color attribute replaces the original Priority-Color attribute of BGP routes.

Usage guidelines

The Priority-Color extended community attribute is used only in SDWAN-encapsulated EVPN routes. In an SDWAN network, you can add backup routes for an EVPN route by adding the Priority-Color extended community attribute. When the data channel fails, traffic can bypass the data channel.

If an IP prefix advertisement route does not contain a Priority-Color attribute, only one route can be added to the BGP-VPN instance routing table or the VPN instance IP routing table. The route's next hop is the next hop of the IP prefix advertisement route. If the next hop is not reachable, the IP prefix advertisement route fails, and thus traffic forwarding to the IP prefix fails.

If an IP prefix advertisement route contains Priority-Color attributes, the device can add one primary route and multiple backup routes to the BGP-VPN instance routing table as follows:

- If the Priority-Color attributes contain device IDs, the device generates a backup route based on each Priority-Color attribute.
- If the Priority-Color attributes do not contain device IDs, the device generates a backup route based on each SDWAN device in the site identified by the site ID in each Priority-Color attribute.

The primary and backup routes use the same prefix. When a backup route is added to the VPN instance IP routing table, the next hop is the system IP of the device identified by the site ID and device ID in the Priority-Color attribute.

When the primary route is reachable, the primary route is added to the VPN instance IP routing table. When the primary route fails, the optimal backup route is added to the VPN instance IP routing table. The optimal backup route is determined as follows:

1. The backup route with the highest priority is the optimal backup route. The priority of a backup route is determined by the priority value in the Priority-Color attribute that generated the backup route. A smaller priority value indicates a higher priority.
2. If multiple backup routes have the same priority, the backup route with the lowest next hop IP address is the optimal route.

In BGP-VPN IPv4 or IPv6 unicast address family, you can enable BGP load balancing by using the **balance** command. All optimal backup routes with the same priority are then added to the VPN instance IP routing table for load balancing, regardless of the primary route's state.

In BGP load balancing, the priority value of the primary route is regarded as 0. The primary route and the backup routes with priority value of 0 are all added to the VPN instance IP routing table for load balancing. When the primary route fails, the primary route does not participate in load balancing any

longer. If no backup routes with priority value of 0 exist, only the primary route is added to the VPN instance IP routing table and no load balancing can be performed. After the primary route fails, all backup routes with the same, smallest priority value are added to the VPN instance IP routing table for load balancing.

For more information about BGP load balancing, see BGP configuration in *Layer 3—IP Routing Configuration Guide*.

When you specify a Priority-Color extended community attribute in *Priority:Site ID:Device ID* format, the attribute cannot take effect if it has the same site ID as an existing Priority-Color extended community attribute in *Priority:Site ID* format.

Examples

Configure node 10 in **permit** mode for routing policy **policy1** to add Priority-Color extended community attribute 1:10:10 to BGP routes.

```
<Sysname> system-view
```

```
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy-policy1-10] apply extcommunity priority-color 1:10:10 additive
```

New feature: Configuring automatic SIM registration

Configuring automatic SIM registration

With automatic SIM registration enabled, when a new SIM is inserted into the device, the device will, within five minutes, send a registration request to the service provider's registration server and report device information and SIM information to the server.

After an SSL client policy is configured, the device will use the SSL parameters specified in the SSL client policy to establish an HTTPS connection with the registration server. Only after the device is authenticated by the registration server, it can register with the server and report device information and SIM information to the server. For information about configuring an SSL client policy, see SSL configuration in *Security Configuration Guide*.

- If the registration succeeds, the device saves the ICCID and registration time of the SIM, and re-registers with the server every 30 days.
- If the registration fails, the device saves the ICCID and registration time of the SIM card, and resends a registration request to service provider's registration server at 1-hour intervals until the registration succeeds or the registration fails for 10 consecutive times.

Restrictions and guidelines

This feature is supported only on a 5G modem.

Procedure

1. Enter system view.

system-view

2. Specify a registration server by its IP address or domain name.

sim register server { **hostname** *name* | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }
[**port** *port-number*]

By default, no registration server is specified.

3. Specify an SSL client policy for SIM registration.

sim register ssl-client-policy *policy-name*

By default, no SSL client policy is configured for SIM registration.

4. Enable automatic SIM registration.

sim register enable

By default, automatic SIM registration is disabled.

Command reference

display sim register

Use **display sim register** to display automatic SIM registration information.

Syntax

Use **display sim register** to display automatic SIM registration information.

Syntax

sim register enable

Use **sim register enable** to enable automatic SIM registration.

Use **undo sim register enable** to disable automatic SIM registration.

Syntax

sim register enable

undo sim register enable

Default

Automatic SIM registration is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With automatic SIM registration enabled, when a new SIM is inserted into the device, the device will, within five minutes, send a registration request to the service provider's registration server and report device information and SIM information to the server.

- If the registration succeeds, the device saves the ICCID and registration time of the SIM card, and re-registers with the server every 30 days.
- If the registration fails, the device saves the ICCID and registration time of the SIM card, and resends a registration request to service provider's registration server at 1-hour intervals until the registration succeeds or the registration fails for 10 consecutive times.

This feature is supported only on a 5G modem.

Examples

```
# Enable automatic SIM registration.
```

```
<Sysname> system-view
```

```
[Sysname] sim register enable
```

Related commands

sim register server

sim register server

Use **sim register server** to specify a registration server.

Use **undo sim register server** to restore the default.

Syntax

sim register server { **hostname** *name* | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*]

undo sim register server

Default

No registration server is specified.

Views

System view

Predefined user roles

network-admin

Parameters

hostname *name*: Specifies the registration server by its domain name. The value is case sensitive.

ipv4 *ipv4-address*: Specifies the registration server by its IPv4 address.

ipv6 *ipv6-address*: Specifies the registration server by its IPv6 address.

port *port-number*: Specifies the port number the registration server listens on. The value range for the *port-number* argument is 1024 to 65535. The default value is 9999.

Usage guidelines

After you specify a registration server and enable SIM registration, the device sends a registration request to the specified registration server if a new SIM is inserted or a SIM is replaced.

This feature is supported only on a 5G modem.

Examples

Specify the registration server with domain name **example.com** and configure the server to listens on port 10000.

```
<Sysname> system-view
```

```
[Sysname] sim register server hostname example.com port 10000
```

Related commands

display sim register

sim register enable

sim register ssl-client-policy

sim register ssl-client-policy

Use **sim register ssl-client-policy** to configure an SSL client policy for automatic SIM registration.

Use **undo sim register ssl-client-policy** to restore the default.

Syntax

sim register ssl-client-policy *policy-name*

undo sim register ssl-client-policy

Default

No SSL client policy is configured for automatic SIM registration.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL client policy, a case-insensitive string of 1 to 31 characters.

Usage guidelines

After this command is configured, the device uses the SSL parameters specified in the SSL client policy to establish an HTTPS connection with the registration server. The SIM registration requests are sent to the registration server through the HTTPS connection. Only after the device is authenticated by the registration server, it can register with the server and report device information and SIM information to the server. For information about configuring an SSL client policy, see SSL configuration in *Security Configuration Guide*.

This feature is supported only on a 5G modem.

Examples

Specify SSL client policy **policy1** for SIM card registration.

```
<Sysname> system-view
```

```
[Sysname] sim register ssl-client-policy policy1
```

Related commands

display ssl client-policy (See SSL commands in *Security Command Reference*)

ssl client-policy (See SSL commands in *Security Command Reference*)

New feature: Configuring TCP congestion control algorithm for TCP proxy

Configuring TCP congestion control algorithm for TCP proxy

About this task

When you perform this task, you can configure one of the following TCP congestion control algorithms:

- **Reno**—Use this algorithm in scenarios with low latency and low bandwidth. In scenarios with high latency and high bandwidth, the speed of data transmission takes a long time to reach the maximum and thus the bandwidth utilization rate is low.
Reno is an early TCP congestion control algorithm that increases the number of congestion windows on receipt of ACK messages.
- **BIC**—Use this algorithm in scenarios with high bandwidth and low packet loss ratio.
BIC can make good use of remaining bandwidth resources and improve throughput, because this algorithm does not slow down packet sending as long as no packet loss occurs. However, the transmission latency of this algorithm is high. This algorithm will reduce the number of congestion windows when transmission errors cause packet loss.

- **BBR**—Use this algorithm in scenarios with high bandwidth, high latency, and packet loss.
BBR does not use packet loss as a congestion signal. In a scenario with high packet loss ratio, this algorithm can ensure high throughput and reduce transmission latency effectively. BBRv2 improves intra-protocol fairness by balancing aggressiveness.

Restrictions and guidelines

This task does not take effect on the modules that support TCP congestion control algorithm configuration. The TCP congestion control algorithm used by such a module depends on its configuration. For example, you can use the **waas tfo congestion-method** command to specify a TCP congestion control algorithm for the WAN side in the WAAS module.

The modules that do not support TCP congestion control algorithm configuration use the same algorithm as the TCP proxy module.

Procedure

1. Enter system view.
system-view
2. Specify a TCP congestion control algorithm for TCP proxy.
tcp-proxy congestion-method { bbrv1 | bbrv2 | bic | reno }
By default, the TCP congestion control algorithm is Reno for TCP proxy.

Command reference

tcp-proxy congestion-method

Use **tcp-proxy congestion-method** to specify a TCP congestion control algorithm for TCP proxy.

Use **undo tcp-proxy congestion-method** to restore the default.

Syntax

tcp-proxy congestion-method { bbrv1 | bbrv2 | bic | reno }
undo tcp-proxy congestion-method

Default

The TCP congestion control algorithm is Reno for TCP proxy.

Views

System view

Predefined user roles

network-admin

Parameters

bbrv1: Specifies BBRv1 as the TCP congestion control algorithm.

bbrv2: Specifies BBRv2 as the TCP congestion control algorithm.

bic: Specifies BIC as the TCP congestion control algorithm.

reno: Specifies Reno as the TCP congestion control algorithm.

Usage guidelines

This command does not take effect on the modules that support TCP congestion control algorithm configuration. The TCP congestion control algorithm used by such a module depends on its

configuration. For example, in the WAAS module, you can use the **waas tfo congestion-method** command to specify a TCP congestion control algorithm for the WAN side.

The modules that do not support TCP congestion control algorithm configuration use the same algorithm as the TCP proxy module.

When you use this command, you can configure one of the following TCP congestion control algorithms:

- **Reno**—Use this algorithm in scenarios with low latency and low bandwidth. In scenarios with high latency and high bandwidth, the speed of data transmission takes a long time to reach the maximum and thus the bandwidth utilization rate is low.
Reno is an early TCP congestion control algorithm that increases the number of congestion windows on receipt of ACK messages.
- **BIC**—Use this algorithm in scenarios with high bandwidth and low packet loss ratio.
BIC can make good use of remaining bandwidth resources and improve throughput, because this algorithm does not slow down packet sending as long as no packet loss occurs. However, the transmission latency of this algorithm is high. This algorithm will reduce the number of congestion windows when transmission errors cause packet loss.
- **BBR**—Use this algorithm in scenarios with high bandwidth, high latency, and packet loss.
BBR does not use packet loss as a congestion signal. In a scenario with high packet loss ratio, this algorithm can ensure high throughput and reduce transmission latency effectively. BBRv2 improves intra-protocol fairness by balancing aggressiveness.

Examples

```
# Specify Reno as the TCP congestion control algorithm for TCP proxy.  
<Sysname> system-view  
[Sysname] tcp-proxy congestion-method reno
```

Related commands

waas tfo congestion-method (*Layer 3—IP Services Command Reference*)

New feature: Specifying the longest match principle for next hop recursion

Specifying the longest match principle for next hop recursion

About this task

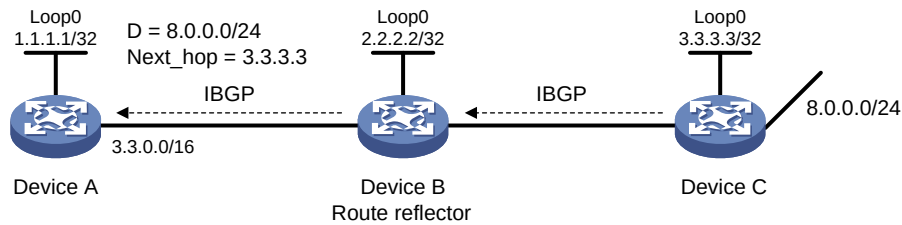
By default, BGP first looks up in its directly connected routes for a recursive route during a route recursion. If no matching routes exist, BGP will look up in routes generated by all routing protocols based on the longest match principle. The device considers the next hop of a received BGP route as directly connected when the next hop belongs to the same subnet as a direct route. As a result, packet forwarding failure will occur when the device uses this BGP route to forward matching packets.

As shown in [Figure 39](#), Device B has established an IBGP session to Device A and Device C respectively. All devices use a loopback interface as the source port for TCP connection. On receipt of BGP route 8.0.0.0/24 from Device C, Device B reflects the route to Device A. The addresses of the interfaces that connect Device A and Device B belong to subnet 3.3.0.0/16.

If the next hop information exchanged between IBGP peers remains unchanged, the next hop of BGP route 8.0.0.0/24 is 3.3.3.3. Device A considers 3.3.3.3 as a directly connected next hop

because 3.3.3.3 belongs to subnet 3.3.0.0/16 and a direct route to 3.3.0.0/16 exists. Packet forwarding failure will occur if Device A forwards packets destined for subnet 8.0.0.0/24 over 3.3.3.3.

Figure 39 Next hop recursion error



To resolve this issue, you can specify the longest match principle for next hop recursion to ensure the recursive route is reachable. BGP will directly look up in routes generated by all routing protocols and select a matching route based on the longest match principle.

Procedure (IPv4 unicast)

1. Enter system view.
system-view
2. Enter BGP IPv4 unicast address family view or BGP-VPN IPv4 unicast address family view.
 - o Execute the following commands in sequence to enter BGP IPv4 unicast address family view:


```
bgp as-number [ instance instance-name ]
```

```
address-family ipv4 [ unicast ]
```
 - o Execute the following commands in sequence to enter BGP-VPN IPv4 unicast address family view:


```
bgp as-number [ instance instance-name ]
```

```
ip vpn-instance vpn-instance-name
```

```
address-family ipv4 [ unicast ]
```
3. Specify the longest match principle for BGP next hop recursion.


```
nexthop recursive-lookup longest-match [ route-policy route-policy-name ]
```

By default, BGP first looks up in its directly connected routes for a recursive route during a route recursion.

This command applies to all BGP routes received from peers in one of the following scenarios:

 - o The **route-policy** *route-policy-name* option is not specified.
 - o The specified routing policy does not exist.

Procedure (IPv6 unicast)

1. Enter system view.
system-view
2. Enter BGP IPv6 unicast address family view or BGP-VPN IPv6 unicast address family view.
 - o Execute the following commands in sequence to enter BGP IPv6 unicast address family view:


```
bgp as-number [ instance instance-name ]
```

```
address-family ipv6 [ unicast ]
```
 - o Execute the following commands in sequence to enter BGP-VPN IPv6 unicast address family view:


```
bgp as-number [ instance instance-name ]
```

ip vpn-instance *vpn-instance-name*

address-family ipv6 [**unicast**]

3. Specify the longest match principle for BGP next hop recursion.

nexthop recursive-lookup longest-match [**route-policy** *route-policy-name*]

By default, BGP first looks up in its directly connected routes for a recursive route during a route recursion.

This command applies to all BGP routes received from peers in one of the following scenarios:

- The **route-policy** *route-policy-name* option is not specified.
- The specified routing policy does not exist.

Command reference

nexthop recursive-lookup longest-match

Use **nexthop recursive-lookup longest-match** to specify the longest match principle for BGP next hop recursion.

Use **undo nexthop recursive-lookup longest-match** to restore the default.

Syntax

nexthop recursive-lookup longest-match [**route-policy** *route-policy-name*]

undo nexthop recursive-lookup longest-match

Default

By default, BGP first looks up in its directly connected routes for a recursive route during a route recursion. If no matching routes exist, BGP will look up in routes generated by all routing protocols based on the longest match principle.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The default method for next hop recursion might cause packet forwarding failure. The device considers the next hop of a received BGP route as directly connected when the next hop belongs to the same subnet as a direct route. As a result, packet forwarding failure will occur when the device uses this BGP route to forward matching packets.

To resolve this issue, you can use this feature to ensure the recursive route is reachable. BGP will directly look up in routes generated by all routing protocols and select a matching route based on the longest match principle.

The **nexthop recursive-lookup longest-match** command applies to all BGP routes received from peers in one of the following scenarios:

- The **route-policy** *route-policy-name* option is not specified.
- The specified routing policy does not exist.

Examples

Specify the longest match principle to recurse routes that pass routing policy **policy1** in BGP IPv4 unicast address family view.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] address-family ipv4 unicast
```

```
[Sysname-bgp-default-ipv4] nexthop recursive-lookup longest-match route-policy policy1
```

New feature: Configuring POS application load sharing and FEP group backup

Configuring a POS application template group

About this task

Perform this task to create a POS application template group and add POS application templates to the group. POS application load sharing can be realized according to the weight, state, and transaction load of each application template in the POS application template group.

Restrictions and guidelines

An added POS application template must be an existing TCP-based POS application template. If the specified application template does not exist or is not TCP type, the POS application template group can be configured but it does not take effect.

Procedure

1. Enter system view.
system-view
2. Create a POS application template group and enter its view.
posa app-group app-group-name
By default, no POS application template group exists.
3. Add a POS application template to the POS application template group.
app app-id weight weight-value
By default, no POS application template exists in a POS application template group.
4. Specify a backup POS application template group.
backup app-group app-group-name
By default, a POS application template group does not have a backup group.

Command reference

display posa load-sharing statistics

Use **display posa load-sharing statistics** to display load sharing statistics about POS application template groups.

Syntax

display posa load-sharing statistics [**app-group** *app-group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

app-group *app-group-name*: Specifies a POS application template group by its name, a case-insensitive string of 1 to 31 characters. If no application template group is specified, this command displays load sharing statistics about all POS application template groups.

Usage guidelines

The router collects load sharing statistics about POS application template groups every 5 seconds. You can use this command to view the number of transaction request packets successfully sent to the FEPs in the last 5 seconds and since device startup.

After a primary and backup switchover of POS application template groups, the history statistics are still retained.

Examples

Display load sharing statistics about all POS application template groups.

```
<Sysname> display posa load-sharing statistics
```

```
App group: ag1
```

AppID	Weight	Last 5 sec	History
1	30	30	166
2	40	42	178
4	30	31	160
6	80	80	390

```
App group: ag2
```

AppID	Weight	Last 5 sec	History
1	90	90	466
4	60	60	260
8	40	40	190

Display load sharing statistics about POS application template group **ag1**.

```
<Sysname> display posa load-sharing statistics app-group ag1
```

```
App group: ag1
```

AppID	Weight	Last 5 sec	History
1	30	30	166
2	40	42	178

4	30	31	160
6	80	80	390

Table 61 Command output

Field	Description
App group	Name of a POS application template group.
AppID	ID of a POS application template in the POS application template group.
Weight	Weight of the POS application template in load sharing.
Last 5 sec	Number of transaction request packets successfully sent to the FEP in the last 5 seconds.
History	Number of transaction request packets successfully sent to the FEP since device startup.

Related commands

reset posa load-sharing statistics

posa app-group

Use **posa app-group** to create a POS application template group and enter its view, or enter the view of an existing POS application template group.

Use **undo posa app-group** to remove a POS application template group.

Syntax

posa app-group *app-group-name*

undo posa app-group *app-group-name*

Default

No POS application template group exists.

Views

System view

Predefined user roles

network-admin

Parameters

app-group-name: Specifies a POS application template group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A POS application template group can be applied to POS terminal templates operating in transparent mode or POS application mapping entries. Applying a POS application template group can realize load sharing among the POS application templates in the POS application template group.

The router supports a maximum of 1024 application template groups.

Examples

Create POS application template group **ag1** and enter its view.

```
<Sysname> system-view
[Sysname] posa app-group ag1
[Sysname-posa-appgrp-ag1]
```


reset posa load-sharing statistics

Use **reset posa load-sharing statistics** to clear load sharing statistics about POS application template groups.

Syntax

reset posa load-sharing statistics [**app-group** *app-group-name*]

Views

User view

Predefined user roles

network-admin

Parameters

app-group *app-group-name*: Specifies a POS application template group by its name, a case-insensitive string of 1 to 31 characters. If no application template group is specified, this command clears load sharing statistics about all POS application template groups.

Examples

Clear load sharing statistics about POS application template groups.

```
<Sysname> reset posa load-sharing statistics
```

Related commands

display posa load-sharing statistics

New feature: Disabling BGP from flushing specific routes to the routing table

Disabling BGP from flushing specific routes to the routing table

About this task

Perform this task to disable BGP from flushing routes that match the specified routing policy to the routing table.

This feature applies to the following scenarios:

- In an MPLS L3VPN network, all the optimal private BGP routes will be flushed to the routing table of a PE by default. You can configure this feature to prevent unnecessary routes from being flushed to the IP routing table and improve the forwarding performance of the PE.
- In a route reflection network, configure this feature to not flush specific BGP routes to the routing table of the RR. Then, the RR only advertises and receives routes but does not forward service traffic, which saves the system resources of the RR.

Procedure (IPv4 unicast)

1. Enter system view.

system-view

2. Enter BGP IPv4 unicast address family view or BGP-VPN IPv4 unicast address family view.
 - Execute the following commands in sequence to enter BGP IPv4 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv4 [**unicast**]

- Execute the following commands in sequence to enter BGP-VPN IPv4 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

ip vpn-instance *vpn-instance-name*

address-family ipv4 [**unicast**]

3. Disable BGP from flushing routes that match the specified routing policy to the routing table.

routing-table bgp-rib-only [**route-policy** *route-policy-name*]

By default, BGP flushes the optimal routes to the routing table.

Procedure (IPv6 unicast)

1. Enter system view.

system-view

2. Enter BGP IPv6 unicast address family view or BGP-VPN IPv6 unicast address family view.

- Execute the following commands in sequence to enter BGP IPv6 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv6 [**unicast**]

- Execute the following commands in sequence to enter BGP-VPN IPv6 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

ip vpn-instance *vpn-instance-name*

address-family ipv6 [**unicast**]

3. Disable BGP from flushing routes that match the specified routing policy to the routing table.

routing-table bgp-rib-only [**route-policy** *route-policy-name*]

By default, BGP flushes the optimal routes to the routing table.

Command reference

routing-table bgp-rib-only

Use **routing-table bgp-rib-only** to disable BGP from flushing routes that match the specified routing policy to the routing table.

Use **undo routing-table bgp-rib-only** to restore the default.

Syntax

routing-table bgp-rib-only [**route-policy** *route-policy-name*]

undo routing-table bgp-rib-only

Default

BGP flushes the optimal routes to the routing table.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP-VPN IPv4 unicast address family view
BGP-VPN IPv6 unicast address family view
BGP IPv4 flowspec address family view
BGP IPv6 flowspec address family view
BGP-VPN IPv4 flowspec address family view
BGP-VPN IPv6 flowspec address family view

Predefined user roles

network-admin

Parameters

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a routing policy or the specified routing policy does not exist, BGP does not flush any routes to the routing table. The apply clauses in the specified routing policy do not take effect.

Usage guidelines

This command applies to the following scenarios:

- In an MPLS L3VPN network, all the optimal private BGP routes will be flushed to the routing table of a PE by default. You can execute this command to prevent unnecessary routes from being flushed to the IP routing table and improve the forwarding performance of the PE.
- In a route reflection network, execute this command to not flush specific BGP routes to the routing table of the RR. Then, the RR only advertises and receives routes but does not forward service traffic, which saves the system resources of the RR.
- In a flowspec network, flowspec routes matching the routing policy specified in this command will not be processed by QoS.

This command is mutually exclusive with the **advertise-rib-active** command.

Examples

In BGP IPv4 unicast address family view, disable BGP from flushing BGP IPv4 unicast routes that match routing policy **policy1** to the routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] routing-table bgp-rib-only route-policy policy1
```

New feature: Configuring the POS application connection keep feature

Configuring the POS application connection keep feature

About this task

After you configure this feature, when the IP address corresponding to the FEP hostname in the POS application template changes, the POS access device does not disconnect the current TCP connection for the POS application. Instead, it initiates a new connection immediately when it detects the disconnection through TCP keepalive. When the POS access device establishes the new TCP

connection, it selects the IP address of the FEP as follows (the domain name refers to the host name of the FEP):

- If the domain name and IP address mapping saved on the DNS server is not expired, the access device selects the IP address in the mapping.
- If the domain name and IP address mapping saved on the DNS server has expired and the DNS server has no latest domain name and IP address mapping, the access device selects the IP address used to establish the last TCP connection.

Restrictions and guidelines

This feature applies only to the TCP connections between POS application templates and FEPs. Configuring this feature in system view takes effect on all the TCP connections.

Procedure

1. Enter system view.

system-view

2. Configure the uninterrupted connection for a POS terminal.

posa app-connection keep

By default, this feature is not configured. When the IP address corresponding to the host name of an FEP changes, the POS access device will disconnect the POS application template's TCP connection with the FEP, and use the new IP address to establish the TCP connection.

Command reference

posa app-connection keep

Use **posa app-connection keep** to configure the POS access device to keep the TCP connection between a POS application template and an FEP when the IP address for the FEP host name changes.

Use **undo posa app-connection keep** to restore the default.

Syntax

posa app-connection keep

undo posa app-connection keep

Default

When the IP address corresponding to the host name of an FEP changes, the POS access device will disconnect the POS application template's TCP connection with the FEP, and use the new IP address to establish the TCP connection.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command applies only to the TCP connections between POS application templates and FEPs. Execution of this command in system view takes effect on all the TCP connections.

After you execute this command, when the IP address corresponding to the FEP hostname in the POS application template changes, the POS access device does not disconnect the current TCP connection. Instead, it initiates a new connection immediately when it detects the disconnection

through TCP keepalive. When the POS access device establishes the new TCP connection, it selects the IP address of the FEP as follows (the domain name refers to the host name of the FEP):

- If the domain name and IP address mapping saved on the DNS server is not expired, the access device selects the IP address in the mapping.
- If the domain name and IP address mapping saved on the DNS server has expired and the DNS server has no latest domain name and IP address mapping, the access device selects the IP address used to establish the last TCP connection.

After you execute the **undo** command, the POS access device will keep the current connection between the POS application template and the FEP, and when the IP address for the FEP host name changes, the POS access device disconnects the current connection and uses a new IP address to establish a new connection.

Examples

Keep the TCP connection when the IP address for an FEP host name in a POS application template changes.

```
<Sysname> system-view
```

```
[Sysname] posa app-connection keep
```

New feature: RIR-SDWAN

Configuring RIR-SDWAN

Enabling the RIR-SDWAN service

1. Enter system view.
system-view
2. Enable the RIR-SDWAN service and enter RIR-SDWAN view.
rir sdwan

By default, the RIR-SDWAN service is disabled.

Enabling RIR to concern bandwidth when performing link selection

About this task

If the user concerns about forwarding paths of service traffic and does not concern about link quality and bandwidth, you can disable RIR from concerning bandwidth when performing link selection.

Procedure

1. Enter system view.
system-view
2. Enter RIR-SDWAN view.
rir sdwan
3. Enable RIR to concern bandwidth when performing link selection.
link-bandwidth ignore

By default, RIR concerns bandwidth when performing link selection.

Specifying link preference values for links

1. Enter system view.
system-view
2. Enter RIR-SDWAN view.
rir sdwan
3. Enter RIR-SDWAN flow template view.
flow *flow-id*
4. Configure a link preference.
path sdwan transport-network *network-name* [**group-id** *group-id*] **preference** *preference*
By default, no link preference is configured in a flow template.

Enabling the device to preferentially select links of the same transport network

About this task

With this feature enabled, the device preferentially selects a TTE connection with the same transport network name for forwarding packets. If the selected TTE connections do not meet the requirements, the device selects a TTE connection with a different transport network name. If multiple TTE connections with the same transport network name are available, they load share traffic based on link selection principles.

Procedure

1. Enter system view.
system-view
2. Enter RIR-SDWAN view.
rir sdwan
3. Enter RIR-SDWAN flow template view.
flow *flow-id*
4. Enable the device to preferentially select links of the same transport network.
link-select same-transport-network prefer
By default, the device is disabled from preferentially selecting links of the same transport network.

Establishing RIR collaboration relationship between the local and peer devices

About this task

The devices in an RIR collaboration device group must reside in the same site. Each pair of devices in an RIR collaboration device group must establish RIR collaboration relationship. You must configure this command on both the local and peer devices.

In a pair of devices with RIR collaboration relationship, the device with a lower IP address is the client. The client uses the port number specified by using this command to initiate a TCP connection (collaboration channel) request to its peer. Through the collaboration channel, the peer device can send the TTE connection and RIR link quality information of the specified tunnel interface to the local device.

Restrictions and guidelines

The local and peer devices must use the same TCP port number for link data synchronization. A device can use the same or different TCP port numbers to synchronize data to different peers.

If you execute this command multiple times to specify the same local IP address, peer device ID, and peer IP address, the most recent configuration takes effect.

You can configure only one collaboration channel between the local and peer devices. Make sure the IP addresses of the local and peer devices are same type.

Procedure

1. Enter system view.

system-view

2. Establish RIR collaboration relationship between the local and peer devices.

```
sdwan collaboration peer device-id device-id [ vpn-instance vpn-instance-name ]  
{ peer-ipv4-address | peer-ipv6-address } local { local-ipv4-address |  
local-ipv6-address } [ sync-port port-number ]
```

By default, the RIR collaboration relationship is not established between the local and peer devices.

Associating a local SDWAN extended tunnel interface with a peer SDWAN tunnel interface

About this task

After you configure this feature, if the link selection result on the local end is packet forwarding through the peer device TTE connection, the local device forwards data packets as follows:

1. Performs SDWAN extended encapsulation for data packets on the local end.
2. Forwards the packets to the peer device through the SDWAN extended tunnel interface associated with the tunnel interface of the TTE connection.

Procedure

1. Enter system view.

system-view

2. Enter SDWAN extended tunnel view in GRE encapsulation mode.

```
interface tunnel tunnel-number mode sdwan-ex gre [ ipv6 ]
```

3. Associate a local SDWAN extended tunnel interface with a peer SDWAN tunnel interface.

```
sdwan collaboration-map peer-device-id device-id peer-interface-id interface-id
```

By default, a local SDWAN extended tunnel interface is not associated with any SDWAN tunnel interface.

Synchronizing TTE connection and RIR link quality information of the local SDWAN tunnel interface to the peer device through the collaboration channel

1. Enter system view.

system-view

2. Enter SDWAN tunnel interface view.

```
interface tunnel tunnel-number mode sdwan udp
```

3. Synchronize TTE connection and RIR link quality information of the local SDWAN tunnel interface to the peer device through the collaboration channel.

sdwan collaboration peer-device-id *device-id*

By default, TTE connection and RIR link quality information of the local SDWAN tunnel interface are not synchronized to the peer device through the collaboration channel.

Configuring a redirect IP address for RIR data packets

About this task

In the RIR collaboration network, Owners are introduced to RIR for forwarding one service flow through the same RIR collaboration device. RIR calculates a unique Owner by using the quintuple of each service flow. This makes sure that one service flow is forwarded through the same Owner device. For a service flow directly forwarded to the non-Owner collaboration device, configure this command to redirect the service flow to a collaboration device that acts as an Owner.

Procedure

1. Enter system view.

system-view

2. Configure a redirect IP address for RIR data packets.

rir redirect peer *peer-ipv4-address* **interface** *interface-type interface-number*

By default, no redirect IP address is configured for RIR data packets. RIR data packets are not redirected to the peer device.

Configuring an interface RIR collaboration group ID

About this task

In the RIR collaboration network, to forward one service flow through the same Owner device, configure the same interface collaboration group for the interfaces of the collaboration devices accessed by the service flow. For a service flow directly forwarded to the non-Owner collaboration device, it carries the interface collaboration group ID, and is redirected to a collaboration device that acts as an Owner. The Owner device processes the packets on the interface with the same interface collaboration group ID on the local device based on the input interface of the flow.

Procedure

1. Enter system view.

system-view

2. Enter interface view.

interface *interface-type interface-number*

3. Configure an interface RIR collaboration group ID.

rir redirect group *group-id*

By default, no interface RIR collaboration group ID is configured.

Configuring the aging timer for the TTE connection synchronized through the collaboration channel after it is disconnected

1. Enter system view.

system-view

2. Configure the aging timer for the TTE connection synchronized through the collaboration channel after it is disconnected.

sdwan collaboration tte-connection aging aging-time

By default, the aging timer is 180 seconds for the TTE connection synchronized through the collaboration channel after it is disconnected.

Enabling BFD for a tunnel

About this task

This feature can avoid packet forwarding failure when the CPE cannot detect or cannot timely detect SDWAN extended tunnel failure. You need to enable the feature on the CPE devices on both ends of the tunnel. The CPE device periodically sends BFD control packets to the collaboration peer device through the SDWAN extended tunnel. If the device does not receive any BFD control packets from the peer device within five seconds, it sets the tunnel state to Defect. The tunnel interface state is still up. After the SDWAN extended tunnel failure is resolved, the tunnel state is automatically recovered to up.

Procedure

1. Enter system view.
system-view
2. Enter SDWAN extended tunnel view in GRE encapsulation mode.
interface tunnel *tunnel-number* mode sdwan-ex gre [ipv6]
3. Enable BFD for the tunnel.
tunnel bfd enable [*template template-name*]
By default, BFD is disabled for a tunnel.

Configuring application quality detection

About this task

In addition to link quality detection, RIR-SDWAN supports application quality detection. For specific service flows forwarded through the SDWAN tunnels, RIR-SDWAN detects the quality of the application flows with the specified packet signatures.

With this feature enabled, the device uses iNQA to periodically detect the application flows with the specified packet signatures for application quality calculation. The application quality detection result is used for application analysis and does not affect link selection.

Restrictions and guidelines

If application quality detection is enabled, the device does not support the per-packet load balancing mode.

You can specify only one packet signature for an application quality detection instance. To detect applications with multiple packet signatures, create multiple application quality detection instances.

This feature requires creating the same application quality detection instance (with the same name) on the two SDWAN devices. In addition, you must specify the instances as the source and destination instances, respectively, and configure the same signature and quality probe interval settings for the instances.

For a specific service flow, the device does not detect the quality of an application flow without any packets matching the specified signature.

To modify the settings of an application quality detection instance, first disable application quality detection for all service flows of the instance.

The device supports creating application quality detection instances for a maximum of 256 service flows.

Prerequisites

Before enabling application quality detection for a service flow, make sure an associated flow template has been created on the device. Without the configuration, application quality detection cannot take effect on the service flow.

Procedure

1. Enter system view.
system-view
2. Enter RIR-SDWAN view.
rir sdwan
3. Enter application quality detection view.
application-quality
4. Create an application quality detection instance and enter application quality detection instance view.
instance *instance-name*
5. Configure the application quality detection interval.
probe interval *interval*
By default, the application quality detection interval is 60 seconds.
6. Configure the peer device for application quality detection.
peer { **source** | **destination** } **site-id** *site-id* **device-id** *device-id*
By default, no peer device is configured for application quality detection.
7. Configure the packet signature for application quality detection.
signature { **source-ip** { **any** | *src-ip-address* [*src-mask-length*] } **destination-ip** { **any** | *dest-ip-address* [*dest-mask-length*] } | **source-ipv6** { **any** | *src-ipv6-address* [*src-prefix-length*] } **destination-ipv6** { **any** | *dest-ipv6-address* [*dest-prefix-length*] } }
By default, no packet signature is configured for application quality detection.
8. Enable application quality detection for a service flow.
probe flow *flow-id*
By default, application quality detection is disabled for all service flows.
The device supports enabling application quality detection for multiple service flows in an application quality detection instance.
You cannot enable application quality detection for the same service flow in multiple application quality detection instances.

Command reference

New command: application-quality

Use **application-quality** to enter application quality detection view.

Use **undo client enable** to delete the application quality detection view and all its settings.

Syntax

application-quality

undo application-quality

Default

No settings exist in application quality detection view.

Views

RIR-SDWAN view

Predefined user roles

network-admin

Usage guidelines

RIR-SDWAN supports the following detection methods:

- **Link quality detection**—Detects the quality of SDWAN tunnels. RIR-SDWAN performs link selection based on the quality detection result.
- **Application quality detection**—For specific service flows forwarded through the SDWAN tunnels, RIR-SDWAN detects the quality of the application flows with the specified packet signatures for application analysis.

Application quality detection settings must be configured in application quality detection view.

If application quality detection is enabled, the device does not support the per-packet load balancing mode.

Examples

Enter application quality detection view.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] application-quality
[Sysname-rir-sdwan-app]
```

New command: cqi-weight

Use **cqi-weight** to configure the weights for the delay, jitter, and packet loss metrics used for computing CQI values.

Use **undo cqi-weight** to restore the default.

Syntax

cqi-weight delay *delay-weight* **jitter** *jitter-weight* **packet-loss** *packet-loss-weight*
undo cqi-weight

Default

The weights for the delay, jitter, and packet loss metrics are all 1.

Views

RIR-SDWAN flow template view

Predefined user roles

network-admin

Parameters

delay *delay-weight*: Sets the weight for the delay metric used for computing CQI values, in the range of 0 to 10.

jitter *jitter-weight*: Sets the weight for the jitter metric used for computing CQI values, in the range of 0 to 10.

packet-loss *packet-loss-weight*: Sets the weight for the packet loss metric used for computing CQI values, in the range of 0 to 10.

Usage guidelines

RIR-SDWAN computes Comprehensive Quality Indicator (CQI) values to evaluate link quality.

- If the probe result of a metric (delay, jitter, or packet loss rate) is lower than or equal to the associated quality threshold in the SLA, the CQI value for the metric is 100.
- If the probe result of a metric is higher than the associated quality threshold in the SLA, the CQI value for the metric is calculated with the formula: (metric threshold × 100) / probe result of the metric.
- The overall CQI value is calculated with the formula: (x × Ds + y × Js + z × Ls) / (x + y + z).

In this formula, x, y, and z represent the weight values of delay, jitter, and packet loss rate, respectively (the weight values are in the range of 0 to 10, and cannot be all 0). Ds, Js, and Ls represent the CQI values for delay, jitter, and packet loss rate.

To avoid frequent link switchovers, the device uses the approximate overall CQI value to evaluate link quality. The approximate overall CQI value is a multiple of 5 that is smaller than and closest to the overall CQI value. For example, if the overall CQI value is 82.5, the approximate overall CQI value is 80.

For quality tolerant link selection, The device selects the link with the highest approximate overall CQI value as the optimal link. If multiple links have the highest approximate overall CQI value, the device selects one or multiple optimal links from them based on the link load balancing mode.

The weights for the delay, jitter, and packet loss metrics cannot be all 0.

Examples

Configure the weight values for the delay, jitter, and packet loss metrics as 2, 5, and 7, respectively, to compute CQI values for link quality evaluation of flow 1.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] flow 1
[Sysname-rir-sdwan-flow-1] cqi-weight delay 2 jitter 5 packet-loss 7
```

New command: delay threshold

Use **delay threshold** to set the link delay threshold.

Use **undo delay threshold** to restore the default.

Syntax

delay threshold *threshold-value*

undo delay threshold

Default

The link delay threshold is 10 milliseconds.

Views

RIR-VXLAN SLA view

RIR-SDWAN SLA view

Predefined user roles

network-admin

Parameters

threshold-value: Sets the link delay threshold, in the range of 10 to 60000 milliseconds.

Usage guidelines

Link delay refers to the interval between the sending time and receiving time of a packet.

The shorter the delay time, the higher the link quality.

A flow template uses the link delay threshold in its associated SLA to filter links that meet the link delay requirement.

Examples

In SLA 1, set the link delay threshold to 1000 milliseconds for RIR-VXLAN.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] sla 1
[Sysname-rir-sla-1] delay threshold 1000
```

In SLA 1, set the link delay threshold to 1000 milliseconds for RIR-SDWAN.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] sla 1
[Sysname-rir-sdwan-sla-1] delay threshold 1000
```

New command: display rir sdwan application-quality

Use **display rir sdwan application-quality** to display application quality detection information.

Syntax

display rir sdwan application-quality instance *instance-name* [**flow-id** *flow-id*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

instance *instance-name*: Specifies an application quality detection instance by its name, a case-sensitive string of 1 to 63 characters.

flow-id *flow-id*: Specifies a flow template by its flow ID in the range of 1 to 65535. If you do not specify a flow ID, this command displays application quality detection information for all flow templates in the specified instance.

Usage guidelines

This command displays only the application quality detection information within the most recent 10 probe intervals.

Examples

Display application quality detection information for all flow templates in instance **abc**.

```
<Sysname> display rir sdwan application-quality instance abc
Flow ID: 1
Tunnell
Peer TTE: Site ID=1    Device ID=2    Interface ID=4
Period started at      PktCount      Timestamp (msec)
2020/11/16 14:28:00    100          1596273655
```

2020/11/16 14:27:00	100	1596273655
2020/11/16 14:26:00	100	1596273655
2020/11/16 14:25:00	100	1596273655
2020/11/16 14:24:00	100	1596273655
2020/11/16 14:23:00	100	1596273655
2020/11/16 14:22:00	100	1596273655
2020/11/16 14:21:00	100	1596273655
2020/11/16 14:20:00	100	1596273655
2020/11/16 14:19:00	100	1596273655

Peer TTE: Site ID=1 Device ID=2 Interface ID=5

Period started at	PktCount	Timestamp (msec)
2020/11/16 14:28:00	100	1596273655
2020/11/16 14:27:00	100	1596273655
2020/11/16 14:26:00	100	1596273655
2020/11/16 14:25:00	100	1596273655
2020/11/16 14:24:00	100	1596273655
2020/11/16 14:23:00	100	1596273655
2020/11/16 14:22:00	100	1596273655
2020/11/16 14:21:00	100	1596273655
2020/11/16 14:20:00	100	1596273655
2020/11/16 14:19:00	100	1596273655

Flow ID: 2

Tunnel2

Peer TTE: Site ID=1 Device ID=2 Interface ID=3

Period started at	PktCount	Timestamp (msec)
2020/11/16 14:28:00	100	1596273655
2020/11/16 14:27:00	100	1596273655
2020/11/16 14:26:00	100	1596273655
2020/11/16 14:25:00	100	1596273655
2020/11/16 14:24:00	100	1596273655
2020/11/16 14:23:00	100	1596273655
2020/11/16 14:22:00	100	1596273655
2020/11/16 14:21:00	100	1596273655
2020/11/16 14:20:00	100	1596273655
2020/11/16 14:19:00	100	1596273655

Peer TTE: Site ID=1 Device ID=2 Interface ID=6

Period started at	PktCount	Timestamp (msec)
2020/11/16 14:28:00	100	1596273655
2020/11/16 14:27:00	100	1596273655
2020/11/16 14:26:00	100	1596273655
2020/11/16 14:25:00	100	1596273655
2020/11/16 14:24:00	100	1596273655
2020/11/16 14:23:00	100	1596273655
2020/11/16 14:22:00	100	1596273655
2020/11/16 14:21:00	100	1596273655
2020/11/16 14:20:00	100	1596273655
2020/11/16 14:19:00	100	1596273655

Table 62 Command output

Field	Description
Flow ID	Flow template ID.
Tunnel <i>tunnel-number</i>	SDWAN tunnel interface name.
Peer TTE	Peer Transport Tunnel Endpoint (TTE) information of the SDWAN tunnel.
Site ID	Peer TTE site ID of the SDWAN tunnel.
Device ID	Peer TTE device ID of the SDWAN tunnel.
Interface ID	Peer TTE interface ID of the SDWAN tunnel.
Period started at	Start time of the quality detection interval.
PktCount	Number of packets collected within the interval.
Timestamp (msec)	Timestamp (in milliseconds) when the device processed packets with the specified signature within the interval. The timestamp can be used to compute the delay.

New command: display rir sdwan bandwidth tunnel

Use **display rir sdwan bandwidth tunnel** to display bandwidth information for the specified SDWAN tunnel interface and the associated physical output interface.

Syntax

display rir sdwan bandwidth tunnel *tunnel-number*

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

tunnel-number: Specifies an SDWAN tunnel interface by its tunnel interface number.

Examples

Display bandwidth information for interface **Tunnel 1** and the associated physical output interface.

```
<Sysname> display rir sdwan bandwidth tunnel 1
```

Tunnel bandwidth info:

Interface	Total bandwidth	Remaining bandwidth	Bandwidth usage
Tunnel1	200 kbps	200 kbps	0 %

Output interface bandwidth info:

PeerTTE: SiteID=1 DeviceID=2 IfID=2

Interface	Total bandwidth	Remaining bandwidth	Bandwidth usage
GE1/0/1	200 kbps	200 kbps	0 %

PeerTTE: SiteID=1 DeviceID=2 IfID=3

Interface	Total bandwidth	Remaining bandwidth	Bandwidth usage
GE1/0/2	200 kbps	200 kbps	0 %

Table 63 Command output

Field	Description
Tunnel bandwidth info	Tunnel interface bandwidth information.
Interface	Interface name.
Total bandwidth	Total bandwidth of the tunnel interface or the associated physical output interface, in Kbps. The value is the expected bandwidth of the interface.
Remaining bandwidth	Remaining bandwidth of the tunnel interface or the associated physical output interface, in Kbps.
Bandwidth usage	Bandwidth usage of the tunnel interface or the associated physical output interface.
Output interface bandwidth info	Output interface bandwidth information.
PeerTTE	Peer TTE information of the SDWAN tunnel.
SiteID	Peer TTE site ID of the SDWAN tunnel.
DeviceID	Peer TTE device ID of the SDWAN tunnel.
IfID	Peer TTE interface ID of the SDWAN tunnel.

New command: display rir sdwan flow

Use **display rir sdwan flow** to display link selection policy information for the specified service flow.

Syntax

display rir sdwan flow *flow-id*

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

flow-id: Specifies a flow template by its flow ID in the range of 1 to 65535.

Examples

Display link selection information for all available SDWAN tunnels in flow template 1.

```
<Sysname> display rir sdwan flow 1
Flow ID: 1
Session expected bandwidth: 2000 kbps
Quality policy: Yes
Tunnels with different preference values:
  Preference: 8
    Tunnel1
      Site ID   Device ID   Interface ID   CQI
      100       1           100            80
      100       2           110            90
    Tunnel2
```


Site ID	Device ID	Interface ID	CQI
100	1	100	80
100	2	110	90

Preference: 10

Tunnel2

Site ID	Device ID	Interface ID	CQI
100	3	80	80
100	4	120	90

Table 64 Command output

Field	Description
Flow ID	Flow template ID.
Session expected bandwidth	Configured session expected bandwidth, in Kbps.
Quality policy	Quality policy status: Yes—A quality policy is configured. No—No quality policy is configured.
Tunnels with different preference values	Information about SDWAN tunnels with different preferences.
Preference	SDWAN tunnel preference. The smaller the value, the higher the preference.
Tunnel <i>tunnel-number</i>	SDWAN tunnel interface name.
Site ID	Peer TTE site ID of the SDWAN tunnel.
Device ID	Peer TTE device ID of the SDWAN tunnel.
Interface ID	Peer TTE interface ID of the SDWAN tunnel.
CQI	Approximate overall CQI value of the SDWAN tunnel.

New command: display rir sdwan link-quality

Use **display rir sdwan link-quality** to display link quality detection information for SDWAN tunnels.

Syntax

display rir sdwan link-quality [**tunnel** *tunnel-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

tunnel *tunnel-number*: Specifies an SDWAN tunnel interface by its tunnel interface number. If you do not specify this option, the command displays link quality detection information for all SDWAN tunnels.

Usage guidelines

This command displays only the link quality detection information for SDWAN tunnels within the most recent 10 probe intervals.

Examples

Display link quality detection information for all SDWAN tunnels.

```
<Sysname> display rir sdwan link-quality
```

Tunnel1

Peer TTE: Site ID=1	Device ID=2	Interface ID=3	Connectivity: Connected
Period started at	PktLoss (per mill)	Delay (msec)	Jitter (msec)
2020/11/16 14:28:00	0	0	0
2020/11/16 14:27:00	0	0	0
2020/11/16 14:26:00	0	0	0
2020/11/16 14:25:00	0	0	0
2020/11/16 14:24:00	0	0	0
2020/11/16 14:23:00	0	0	0
2020/11/16 14:22:00	0	0	0
2020/11/16 14:21:00	0	0	0
2020/11/16 14:20:00	0	0	0
2020/11/16 14:19:00	0	0	0

Peer TTE: Site ID=1	Device ID=2	Interface ID=4	Connectivity: Connected
Period started at	PktLoss (per mill)	Delay (msec)	Jitter (msec)
2020/11/16 14:28:00	0	0	0
2020/11/16 14:27:00	0	0	0
2020/11/16 14:26:00	0	0	0
2020/11/16 14:25:00	0	0	0
2020/11/16 14:24:00	0	0	0
2020/11/16 14:23:00	0	0	0
2020/11/16 14:22:00	0	0	0
2020/11/16 14:21:00	0	0	0
2020/11/16 14:20:00	0	0	0
2020/11/16 14:19:00	0	0	0

Tunnel2

Peer TTE: Site ID=1	Device ID=2	Interface ID=5	Connectivity: Connected
Period started at	PktLoss (per mill)	Delay (msec)	Jitter (msec)
2020/11/16 14:28:00	0	0	0
2020/11/16 14:27:00	0	0	0
2020/11/16 14:26:00	0	0	0
2020/11/16 14:25:00	0	0	0
2020/11/16 14:24:00	0	0	0
2020/11/16 14:23:00	0	0	0
2020/11/16 14:22:00	0	0	0
2020/11/16 14:21:00	0	0	0
2020/11/16 14:20:00	0	0	0
2020/11/16 14:19:00	0	0	0

Peer TTE: Site ID=1	Device ID=2	Interface ID=6	Connectivity: Connected
Period started at	PktLoss (per mill)	Delay (msec)	Jitter (msec)
2020/11/16 14:28:00	0	0	0
2020/11/16 14:27:00	0	0	0

2020/11/16 14:26:00	0	0	0
2020/11/16 14:25:00	0	0	0
2020/11/16 14:24:00	0	0	0
2020/11/16 14:23:00	0	0	0
2020/11/16 14:22:00	0	0	0
2020/11/16 14:21:00	0	0	0
2020/11/16 14:20:00	0	0	0
2020/11/16 14:19:00	0	0	0

Table 65 Command output

Field	Description
Tunnel <i>tunnel-number</i>	SDWAN tunnel interface name.
Peer TTE	Peer TTE information of the SDWAN tunnel.
Site ID	Peer TTE site ID of the SDWAN tunnel.
Device ID	Peer TTE device ID of the SDWAN tunnel.
Interface ID	Peer TTE interface ID of the SDWAN tunnel.
Connectivity	NQA link connectivity probe result of the SDWAN tunnel: • Connected. • Disconnected.
Period started at	Start time of the quality detection interval.
PktLoss (per mill)	Detected packet loss rate (per mill) of the SDWAN tunnel.
Delay (msec)	Detected delay (in milliseconds) of the SDWAN tunnel.
Jitter (msec)	Detected jitter (in milliseconds) of the SDWAN tunnel.

New command: display rir sdwan session-statistics tunnel

Use **display rir sdwan session-statistics tunnel** to display service session statistics for the specified tunnel interface.

Syntax

In standalone mode:

display rir sdwan session-statistics tunnel *interface-number* [**flow** *flow-id*]

In IRF mode:

display rir sdwan session-statistics tunnel *interface-number* [**flow** *flow-id*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-number: Specifies a tunnel interface by its number. The specified tunnel interface must already exist on the device.

flow flow-id: Specifies a flow template by its flow ID, in the range of 1 to 65535. If you do not specify a flow ID, this command displays session statistics for all flow templates.

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information on the master device. (In IRF mode.)

Examples

Display service session statistics for the tunnel interface 1.

```
<Sysname> system-view
[Sysname] display rir sdwan session-statistics tunnel 1
Tunnel interface: Tun1
Flow ID: 3
Collaboration sessions : 0
Local sessions          : 1
Total sessions          : 1
Session statistics:
      SiteID      DeviceID      InterfaceID      SessCount
      10          1            2                1
```

Table 66 Command output

Field	Description
Tunnel interface	Tunnel interface name.
Collaboration sessions	Number of sessions synchronized from the collaboration channel.
Local sessions	Number of local sessions.
Total sessions	Total number of sessions.
SiteID	Peer device site ID of the session.
DeviceID	Peer device ID of the session.
InterfacelD	Peer device interface ID of the session.
SessCount	Number of sessions.

New command: display sdwan collaboration channel

Use **display sdwan collaboration channel** to display collaboration channel status and packet statistics on the device.

Syntax

display sdwan collaboration channel [**peer-device-id** *device-id*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

peer-device-id *device-id*: Specifies a peer device by its ID in the range of 1 to 255. If you do not specify this option, the command displays status and packet statistics of all collaboration channels on the local device.

Examples

Display status and packet statistics of all collaboration channels on the device.

```
<Sysname> display sdwan collaboration channel
Peer device ID      : 2
Peer IP             : 1.1.1.2
Local IP            : 1.1.1.1
VPN instance        : aa
Sync-port           : 1024
Status              : Connected
Total collaboration channels: 1
Packet statistics:
  Input(total)      : 4 packets
    Add tteConnectionPackets : 1
    Delete tteConnectionPackets: 0
    RirDataPackets      : 1
    SmoothStartPackets   : 1
    SmoothEndPackets     : 1
    SmoothDataPackets    : 0
    DropPackets          : 0
  Ouput(total)      : 4 packets
    Add tteConnectionPackers : 1
    Delete tteConnectionPackets: 0
    RirDataPackets      : 1
    SmoothStartPackets   : 1
    SmoothEndPackets     : 1
    SmoothDataPackets    : 0
    DropPackets          : 0
```

Table 67 Command output

Field	Description
Peer IP	IP address of the peer device of the collaboration channel.
Local IP	IP address of the local device of the collaboration channel.
VPN instance	VPN instance to which the collaboration relationship with the peer device belongs. This field displays a hyphen (-) if the collaboration relationship belongs to the public network instance.
Sync-port	TCP port number used for synchronizing link data between the local and peer devices.
Status	Collaboration channel status: • Init. • Connecting. • Checking. • Connected. • Closed.

Total collaboration connections	Number of collaboration channels on the local device.
Input(total)	Total number of packets received through the collaboration channel by the device.
Add tteConnectionPackets	Number of packets carrying the information to add TTE connection.
Delete tteConnectionPackets	Number of packets carrying the information to delete TTE connection.
RirDataPackets	Number of packets carrying RIR data.
SmoothStartPackets	Number of smoothing start packets.
SmoothEndPackets	Number of smoothing end packets.
SmoothDataPackets	Number of packets carrying the TTE connection smoothing information.
DropPackets	Number of discarded packets.
Output(total)	Total number of packets sent through the collaboration channel by the device.

New command: instance

Use **instance** to create an application quality detection instance and enter its view, or enter the view of an existing application quality detection instance.

Use **undo instance** to delete an application quality detection instance.

Syntax

instance *instance-name*

undo instance *instance-name*

Default

No application quality detection instances exist.

Views

Application quality detection view

Predefined user roles

network-admin

Parameters

instance-name: Specifies an application quality detection instance by its name, a case-sensitive string of 1 to 63 characters excluding spaces.

Usage guidelines

To detect the quality of an application flow with the specified packet signature, create the same application quality detection instance (with the same name) on the two SDWAN devices. In addition, you must specify the instances as the source and destination instances, respectively, and configure the same signature and quality probe interval settings for the instances.

You can specify only one packet signature for an application quality detection instance. To detect applications with multiple packet signatures, create multiple application quality detection instances.

You can create a maximum of 16 application quality detection instances.

Examples

Create application quality detection instance **abc** and enter its view.

```

<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] application-quality
[Sysname-rir-sdwan-app] instance abc
[Sysname-rir-sdwan-app-instance-abc]

```

New command: link-select same-transport-network prefer

Use **link-select same-transport-network prefer** to enable the device to preferentially select links of the same transport network.

undo link-select same-transport-network prefer to disable the device from preferentially selecting links of the same transport network.

Syntax

link-select same-transport-network prefer

undo link-select same-transport-network prefer

Default

The device is disabled from preferentially selecting links of the same transport network.

Views

RIR-SDWAN flow template view

Predefined user roles

network-admin

Usage guidelines

With this feature enabled, the device preferentially selects a TTE connection with the same transport network name for forwarding packets. If the selected TTE connections do not meet the requirements, the device selects a TTE connection with a different transport network name. If multiple TTE connections with the same transport network name are available, they load share traffic based on link selection principles.

Examples

Enable the device to preferentially select links of the same transport network.

```

<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] flow 1
[Sysname-rir-sdwan-flow-1] link-select same-transport-network prefer

```

New command: link-bandwidth ignore

Use **link-bandwidth ignore** to enable RIR to concern bandwidth when performing link selection.

Use **undo link-bandwidth ignore** to disable RIR from concerning bandwidth when performing link selection.

Syntax

link-bandwidth ignore

undo link-bandwidth ignore

Default

RIR concerns bandwidth when performing link selection.

Views

RIR-SDWAN view

Predefined user roles

network-admin

Usage guidelines

If the user concerns about forwarding paths of service traffic and does not concern about link quality and bandwidth, you can disable RIR from concerning bandwidth when performing link selection.

Examples

```
# Disable RIR from concerning bandwidth when performing link selection.
```

```
<Sysname> system-view
```

```
[Sysname] rir sdwan
```

```
[Sysname-rir-sdwan] undo link-bandwidth ignore
```

New command: link-quality probe interval

Use **link-quality probe interval** to set the link quality probe interval.

Use **undo link-quality probe interval** to restore the default.

Syntax

link-quality probe interval *interval*

undo link-quality probe interval

Default

The link quality probe interval is 60 seconds.

Views

RIR-SDWAN view

Predefined user roles

network-admin

Parameters

interval: Sets the link quality probe interval, in seconds. Supported values are 30, 60, 300, and 600.

Usage guidelines

After you enable the RIR-SDWAN service, the device periodically probes link quality of all SDWAN tunnels at the specified intervals, and performs link selection based on the probe result.

If you modify the link quality probe interval, the device stops probing the quality of all SDWAN tunnels, and uses the new interval to start probing the link quality of all SDWAN tunnels.

Examples

```
# Set the link quality probe interval to 600 seconds.
```

```
<Sysname> system-view
```

```
[Sysname] rir sdwan
```

```
[Sysname-rir-sdwan] link-quality probe interval 600
```


New command: path sdwan

Use **path sdwan** to configure a link preference for the flow template.

Use **undo path sdwan** to restore the default.

Syntax

```
path sdwan transport-network network-name [ group-id group-id ] preference preference  
undo path sdwan transport-network network-name [ group-id group-id ]
```

Default

No link preference is configured in a flow template.

Views

RIR-SDWAN flow template view

Predefined user roles

network-admin

Parameters

transport-network *network-name*: Specifies a transport network name, a case-sensitive string of 1 to 31 characters that can contain only letters, digits, underscores (_), and dots (.).

group-id *group-id*: Specifies the group ID of the SDWAN tunnel, in the range of 1 to 65535. If no SDWAN tunnel group ID is available, do not specify this option.

preference *preference*: Specifies a link preference in the range of 1 to 255. The smaller the value, the higher the priority.

Usage guidelines

Use this command to assign a link preference to an SDWAN tunnel by its transport network name or group ID in a flow template. To specify the SDWAN tunnel group ID, use the **sdwan group-id** command. RIR preferentially selects links with higher preference.

You can assign the same link preference value to different links in the same flow template.

A flow template supports assigning preference values to a maximum of 64 links.

Examples

```
# Assign preference 1 to the link with transport network name nt1.
```

```
<Sysname> system-view
```

```
[Sysname] rir sdwan
```

```
[Sysname-rir-sdwan] flow 1
```

```
[Sysname-rir-sdwan-flow-1] path sdwan transport-network nt1 preference 1
```

Related commands

sdwan transport-network

New command: peer

Use **peer** to configure the peer device for application quality detection.

Use **undo peer** to delete the peer device for application quality detection.

Syntax

```
peer { source | destination } site-id site-id device-id device-id
```

undo peer

Default

No peer device is configured for application quality detection.

Views

Application quality detection instance view

Predefined user roles

network-admin

Parameters

source: Specifies the peer device as the source device for application quality detection.

destination: Specifies the peer device as the destination device for application quality detection.

site-id *site-id*: Specifies the site ID configured during SDWAN tunnel establishment for the peer device, in the range of 1 to 65535.

device-id *device-id*: Specifies the device ID configured during SDWAN tunnel establishment for the peer device, in the range of 1 to 255.

Usage guidelines

Use this command to specify a pair of peer devices as the source and destination devices for application quality detection. After you execute the **probe flow** command, the device uses iNQA to periodically detect the application flows with the specified packet signatures for application quality calculation. The application quality detection result is used for application analysis and does not affect link selection.

To modify the peer device settings of an instance, first execute the **undo probe flow** command to disable application quality detection for all service flows of the instance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the peer device as the source device for application quality detection, and configure its site ID as 1 and device ID as 2.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] application-quality instance abc
[Sysname-rir-sdwan-app-instance-abc] peer source site-id 1 device-id 2
```

Related commands

probe flow

sdwan device-id

sdwan site-id

New command: probe flow

Use **probe connect** to enable application quality detection for a service flow.

Use **undo probe connect** to disable application quality detection for a service flow.

Syntax

probe flow *flow-id*

undo probe flow [*flow-id*]

Default

Application quality detection is disabled for all service flows.

Views

Application quality detection instance view

Predefined user roles

network-admin

Parameters

flow-id: Specifies a flow template by its flow ID in the range of 1 to 65535. If you do not specify a flow ID, the **undo probe flow** command disables application quality detection for all flow templates.

Usage guidelines

For specific service flows forwarded through the SDWAN tunnel, use this command to detect the quality of the application flows with the specified packet signature (such as source or destination IP address). The application quality detection result is used for application analysis. You can enable application quality detection for multiple flow templates of an instance.

Before configuring this command, make sure you have configured the following settings:

- Create the associated flow template. Without the configuration, application quality detection cannot take effect on the service flow.
- Use the **peer** command to specify the role, site ID, and device ID for the peer device.
- Use the **signature** command to specify the packet signature for application quality detection.

For a specific service flow, the device does not detect the quality of an application flow without any packets matching the specified signature.

You cannot enable application quality detection for the same service flow in multiple application quality detection instances.

Examples

Enable application quality detection for flow template Flow 1.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] application-quality
[Sysname-rir-sdwan-app] instance abc
[Sysname-rir-sdwan-app-instance-abc] peer source site-id 1 device-id 2
[Sysname-rir-sdwan-app-instance-abc] signature source-ip 10.1.1.1 destination-ip
20.1.1.1
[Sysname-rir-sdwan-app-instance-abc] probe flow 1
```

Related commands

flow

peer

signature

New command: probe interval (application quality detection instance view)

Use **probe interval** to set the application quality detection interval.

Use **undo probe interval** to restore the default.

Syntax

probe interval *interval*

undo probe interval

Default

The application quality detection interval is 60 seconds.

Views

Application quality detection instance view

Predefined user roles

network-admin

Parameters

interval: Sets the application quality detection interval. Supported values are 30, 60, 300, and 600 seconds.

Usage guidelines

After you execute the **probe flow** command, the device uses iNQA to detect the application flows with the specified packet signatures at the specified intervals for application quality calculation. The application quality detection result is used for application analysis and does not affect link selection.

To modify the application quality detection interval setting, first execute the **undo probe flow** command to disable application quality detection for all service flows of the instance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the application quality detection interval to 600 seconds for application quality detection instance **abc**.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan] application-quality
[Sysname-rir-sdwan-app] instance abc
[Sysname-rir-sdwan-app-instance-abc] probe interval 600
```

Related commands

probe flow

New command: rir redirect group

Use **rir redirect group** to configure an interface RIR collaboration group ID.

Use **undo rir recirect group** to restore the default.

Syntax

rir redirect group *group-id*

undo rir redirect group

Default

No interface RIR collaboration group ID is configured.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

In the RIR collaboration network, to forward one service flow through the same Owner device, configure the same interface collaboration group for the interfaces of the collaboration devices accessed by the service flow. For a service flow directly forwarded to the non-Owner collaboration device, it carries the interface collaboration group ID, and is redirected to a collaboration device that acts as an Owner. The Owner device processes the packets on the interface with the same interface collaboration group ID on the local device based on the input interface of the flow.

Examples

Configure RIR collaboration group ID 1 for interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-Gigabitethernet 1/0/1] rir redirect group id 1
```

Related commands

rir redirect peer

New command: rir redirect peer

Use **rir redirect peer interface** to configure a redirect IP address for RIR data packets.

Use **undo rir redirect peer interface** to restore the default.

Syntax

rir redirect peer *peer-ipv4-address* **interface** *interface-type interface-number*

undo rir redirect peer *peer-ipv4-address*

Default

No redirect IP address is configured for RIR data packets. RIR data packets are not redirected to the peer device.

Views

System view

Predefined user roles

network-admin

Parameters

peer-ipv4-address: Specifies the IPv4 address of the collaboration peer device for redirecting RIR data packets.

interface *interface-type interface-number*: Specifies an interface for forwarding redirected RIR data packets by its type and number.

Usage guidelines

In the RIR collaboration network, Owners are introduced to RIR for forwarding one service flow through the same RIR collaboration device. RIR calculates a unique Owner by using the quintuple of each service flow. This makes sure that one service flow is forwarded through the same Owner device. For a service flow directly forwarded to the non-Owner collaboration device, configure this command to redirect the service flow to a collaboration device that acts as an Owner.

Examples

Configure the redirect IP address for RIR data packets as 1.1.1.1.

```
<Sysname> system-view
[Sysname] rir redirect peer 1.1.1.1 interface
```

Related commands

rir redirect group id

New command: rir sdwan

Use **rir sdwan** to enable the RIR-SDWAN service and enter RIR-SDWAN view, or directly enter RIR-SDWAN view if the RIR-SDWAN service is already enabled.

Use **undo rir sdwan** to disable the RIR-SDWAN service.

Syntax

rir sdwan

undo rir sdwan

Default

The RIR-SDWAN service is disabled.

Views

System view

Predefined user roles

network-admin

network-operator

Usage guidelines

RIR can be deployed based on VXLAN tunnels or SDWAN tunnels, which are called RIR-VXLAN and RIR-SDWAN, respectively

- For RIR-VXLAN, use the **rir** command to enable the RIR-VXLAN service.
- For RIR-SDWAN, use the **rir sdwan** command to enable the RIR-SDWAN service.

When you enable the RIR-VXLAN or RIR-SDWAN service, the system enables the RIR process. When you disable the RIR-VXLAN or RIR-SDWAN service, the system disables the RIR process.

You cannot enable both the RIR-VXLAN and RIR-SDWAN services.

- To enable the RIR-SDWAN service when the RIR-VXLAN service is enabled, you must first execute the **undo rir** command to disable the RIR-VXLAN service.
- To enable the RIR-VXLAN service when the RIR-SDWAN service is enabled, you must first execute the **undo rir sdwan** command to disable the RIR-SDWAN service.

For RIR-SDWAN, you must enable the RIR-SDWAN service on all SDWAN devices.

Examples

Enable the RIR-SDWAN service and enter RIR-SDWAN view.

```
<Sysname> system-view
[Sysname] rir sdwan
[Sysname-rir-sdwan]
```

New command: signature

Use **signature** to configure the packet signature for application quality detection.

Use **undo signature** to delete the packet signature for application quality detection.

Syntax

```
signature { source-ip { any | src-ip-address [ src-mask-length ] } destination-ip { any | dest-ip-address [ dest-mask-length ] } | source-ipv6 { any | src-ipv6-address [ src-prefix-length ] } destination-ipv6 { any | dest-ipv6-address [ dest-prefix-length ] } }
```

undo signature

Default

No packet signature is configured for application quality detection.

Views

Application quality detection instance view

Predefined user roles

network-admin

Parameters

source-ip { **any** | *src-ip-address* [*src-mask-length*] }: Specifies a source IPv4 address for packets. The **any** keyword represents any source IPv4 address. The *src-ip-address* argument represents the source IPv4 address of packets, in dotted decimal notation. The *src-mask-length* argument represents the length of the subnet mask, in the range of 1 to 32. If you do not specify the *src-mask-length* argument, the command matches the exact source IPv4 address of packets.

destination-ip { **any** | *dest-ip-address* [*dest-mask-length*] }: Specifies a destination IPv4 address for packets. The **any** keyword represents any destination IPv4 address. The *dest-ip-address* argument represents the destination IPv4 address of packets, in dotted decimal notation. The *dest-mask-length* argument represents the length of the subnet mask, in the range of 1 to 32. If you do not specify the *dest-mask-length* argument, the command matches the exact destination IPv4 address of packets.

source-ipv6 { **any** | *src-ipv6-address* [*src-prefix-length*] }: Specifies a source IPv6 address for packets. The **any** keyword represents any source IPv6 address. The *src-ipv6-address* argument represents the source IPv6 address of packets, in colon-separated hexadecimal notation. The *src-prefix-length* argument represents the prefix length of the source IPv6 address, in the range of 1 to 128. If you do not specify the *src-prefix-length* argument, the command matches the exact source IPv6 address of packets.

destination-ipv6 { **any** | *dest-ipv6-address* [*dest-prefix-length*] }: Specifies a destination IPv6 address for packets. The **any** keyword represents any destination IPv6 address. The *dest-ipv6-address* argument represents the destination IPv6 address of packets, in colon-separated hexadecimal notation. The *dest-prefix-length* argument represents the prefix length of the source IPv6 address, in the range of 1 to 128. If you do not specify the *dest-prefix-length* argument, the command matches the exact destination IPv6 address of packets.

Usage guidelines

After you execute the **probe flow** command for specific service flows, the device will detect the quality of the application flows with the specified packet signatures (such as source or destination IP address).

To modify the packet signature settings of an instance, first execute the **undo probe flow** command to disable application quality detection for all service flows of the instance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Configure the packet signature for application quality detection by specifying the source and destination IPv4 addresses for packets as 10.1.1.1 and 20.1.1.1, respectively.
```

```
<Sysname> system-view
```

```
[Sysname] rir sdwan
[Sysname-rir-sdwan] application-quality
[Sysname-rir-sdwan-app] instance abc
[Sysname-rir-sdwan-app-instance-abc] signature source-ip 10.1.1.1 destination-ip
20.1.1.1
```

Related commands

probe flow

New command: sdwan collaboration peer

Use **sdwan collaboration peer** to establish RIR collaboration relationship between the local and peer devices.

Use **undo sdwan collaboration peer device-id** to restore the default.

Syntax

```
sdwan collaboration peer device-id device-id [ vpn-instance vpn-instance-name ]
{ peer-ipv4-address | peer-ipv6-address } local { local-ipv4-address | local-ipv6-address }
[ sync-port port-number ]
```

```
undo sdwan collaboration peer device-id device-id
```

Default

The RIR collaboration relationship is not established between the local and peer devices.

Views

System view

Predefined user roles

network-admin

Parameters

peer-device-id *device-id*: Specifies a peer device by its ID in the range of 1 to 255.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance on which the local and peer devices establish RIR collaboration relationship. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. The specified VPN instance must exist. If the RIR collaboration relationship belongs to the public network, do not specify this option.

peer-ipv4-address: Specifies an RIR collaboration peer by its IPv4 address.

peer-ipv6-address: Specifies an RIR collaboration peer by its IPv6 address.

local-ipv4-address: Specifies the IPv4 address of the local device.

local-ipv6-address: Specifies the IPv6 address of the local device.

sync-port *port-number*: Specifies the TCP port number used by the local and peer devices to synchronize TTE connection and link quality data. The value range for the *port-number* argument is 1024 to 65535. The default value is 2005. Make sure the port number is not used by any other service on the device.

Usage guidelines

The devices in an RIR collaboration device group must reside in the same site. Each pair of devices in an RIR collaboration device group must establish RIR collaboration relationship. You must configure this command on both the local and peer devices.

In a pair of devices with RIR collaboration relationship, the device with a lower IP address is the client. The client uses the port number specified by using this command to initiate a TCP connection

(collaboration channel) request to its peer. Through the collaboration channel, the peer device can send the TTE connection and RIR link quality information of the specified tunnel interface to the local device.

The local and peer devices must use the same TCP port number for link data synchronization. A device can use the same or different TCP port numbers to synchronize data to different peers.

If you execute this command multiple times to specify the same local IP address, peer device ID, and peer IP address, the most recent configuration takes effect.

You can configure only one collaboration channel between the local and peer devices. Make sure the IP addresses of the local and peer devices are same type.

Examples

Establish RIR collaboration relationship between local device 1.1.1.1 and peer device 1.1.1.2 with device ID 10. They use TCP port number 6000 for link data synchronization.

```
<Sysname> system-view
```

```
[Sysname] sdwan collaboration peer device-id 10 1.1.1.2 local 1.1.1.1 sync-port 6000
```

Related commands

collaboration peer local

New command: sdwan collaboration peer-device-id

Use **sdwan collaboration peer-device-id** to synchronize TTE connection and RIR link quality information of the local SDWAN tunnel interface to the peer device through the collaboration channel.

Use **undo sdwan collaboration peer-device-id** to restore the default.

Syntax

sdwan collaboration peer-device-id *device-id*

undo sdwan collaboration peer-device-id

Default

TTE connection and RIR link quality information of the local SDWAN tunnel interface are not synchronized to the peer device through the collaboration channel.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

device-id: Specifies a peer device by its ID in the range of 1 to 255.

Examples

Synchronize TTE connection and RIR link quality information of local SDWAN tunnel interface 1 to the peer device with device ID 10 through the collaboration channel.

```
<Sysname> system-view
```

```
[Sysname] interface Tunnel1 mode sdwan udp
```

```
[Sysname-Tunnel1] sdwan collaboration peer-device-id 10
```

Related commands

sdwan collaboration peer local

New command: **sdwan collaboration tte-connection aging**

Use **sdwan collaboration tte-connection aging** to configure the aging timer for the TTE connection synchronized through the collaboration channel after it is disconnected.

Use **undo sdwan collaboration tte-connection aging** to restore the default.

Syntax

sdwan collaboration tte-connection aging *aging-time*

undo sdwan collaboration tte-connection aging

Default

The aging timer is 180 seconds for the TTE connection synchronized through the collaboration channel after it is disconnected.

Views

System view

Predefined user roles

network-admin

Parameters

aging-time: Specifies an aging timer in the range of 0 to 300 seconds. Value 0 indicates that the TTE connection does not age.

Examples

Configure the aging timer as 3 seconds for the TTE connection synchronized through the collaboration channel after it is disconnected

```
<Sysname> system-view
```

```
[Sysname] sdwan collaboration tte-connection aging 3
```

New command: **sdwan collaboration-map peer-device-id peer-interface-id**

Use **sdwan collaboration-map peer-device-id peer-interface-id** to associate a local SDWAN extended tunnel interface with a peer SDWAN tunnel interface.

Use **undo sdwan collaboration-map peer-device-id** to restore the default.

Syntax

sdwan collaboration-map peer-device-id *device-id* **peer-interface-id** *interface-id*

undo sdwan collaboration-map peer-device-id

Default

A local SDWAN extended tunnel interface is not associated with any SDWAN tunnel interface.

Views

SDWAN extended tunnel interface view

Predefined user roles

network-admin

Parameters

peer-device-id *device-id*: Specifies a peer device by its ID in the same site, in the range of 1 to 255.

peer-interface-id *interface-id*: Specifies an SDWAN tunnel interface on the peer device in the same site by its ID, in the range of 1 to 255.

Usage guidelines

After you configure this command, if the link selection result on the local end is packet forwarding through the peer device TTE connection, the local device forwards data packets as follows:

1. Performs SDWAN extended encapsulation for data packets on the local end.
2. Forwards the packets to the peer device through the SDWAN extended tunnel interface associated with the tunnel interface of the TTE connection.

Examples

Associate local SDWAN extended tunnel interface 1 with peer SDWAN tunnel interface 2.

```
<Sysname> system-view
```

```
[Sysname] interface tunnel 1 mode sdwan-ex gre
```

```
[Sysname-Tunnel1]sdwan collaboration-map peer-device-id 1 peer-interface-id 2
```

New command: tunnel bfd enable

Use **tunnel bfd enable** to enable BFD for a tunnel.

Use **undo tunnel bfd enable** to disable BFD for a tunnel.

Syntax

tunnel bfd enable [**template** *template-name*]

undo tunnel bfd enable [**template** *template-name*]

Default

BFD is disabled for a tunnel.

Views

SDWAN extended tunnel interface view

Predefined user roles

network-admin

Parameters

template *template-name*: Specifies a BFD session parameter template by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a template or specify a nonexistent template, the default BFD session parameters of the device apply.

Usage guidelines

This feature can avoid packet forwarding failure when the CPE cannot detect or cannot timely detect SDWAN extended tunnel failure. You need to enable the feature on the CPE devices on both ends of the tunnel. The CPE device periodically sends BFD control packets to the collaboration peer device through the SDWAN extended tunnel. If the device does not receive any BFD control packets from the peer device within five seconds, it sets the tunnel state to Defect. The tunnel interface state is still up. After the SDWAN extended tunnel failure is resolved, the tunnel state is automatically recovered to up.

Examples

Enable BFD for SDWAN extended tunnel interface Tunnel1.

```
<Sysname> system-view
```

```
[Sysname] interface tunnel 1 mode sdwan-ex gre
[Sysname-Tunnel1] tunnel bfd enable template aa
```

New feature: SaaS path optimization

SaaS path optimization enables the device to select optimal paths for traffic that accesses SaaS applications and adjust the optimal paths accordingly when path quality changes.

SaaS path optimization

SaaS applications

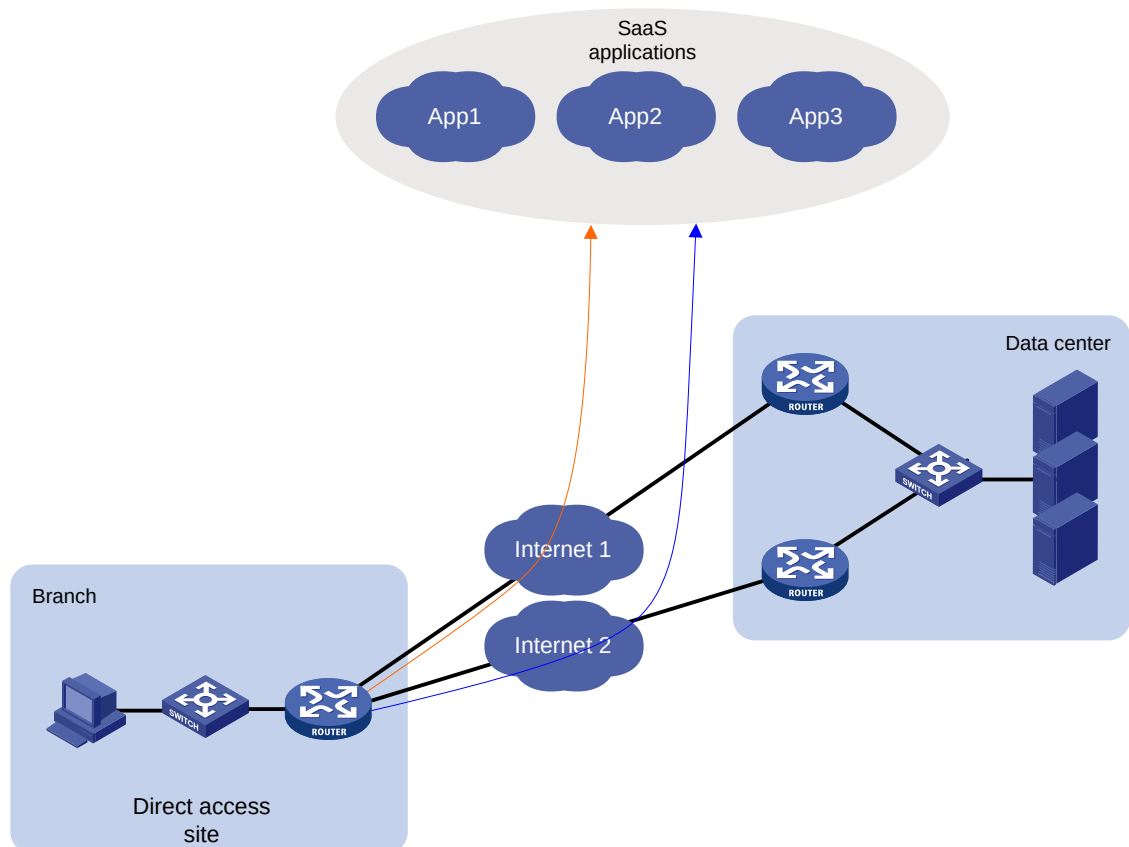
SaaS applications include predefined SaaS applications and user-defined SaaS applications. Typically, predefined SaaS applications are common SaaS applications. User-defined SaaS applications are manually configured to meet service requirements.

Methods for accessing SaaS applications

Direct access

As shown in [Figure 40](#), the device at the branch site can directly access SaaS applications through local interfaces. It performs SaaS path optimization based on local quality information for the paths that can directly access SaaS applications. This access method is supported in both RIR-VXLAN and RIR-SDWAN networks.

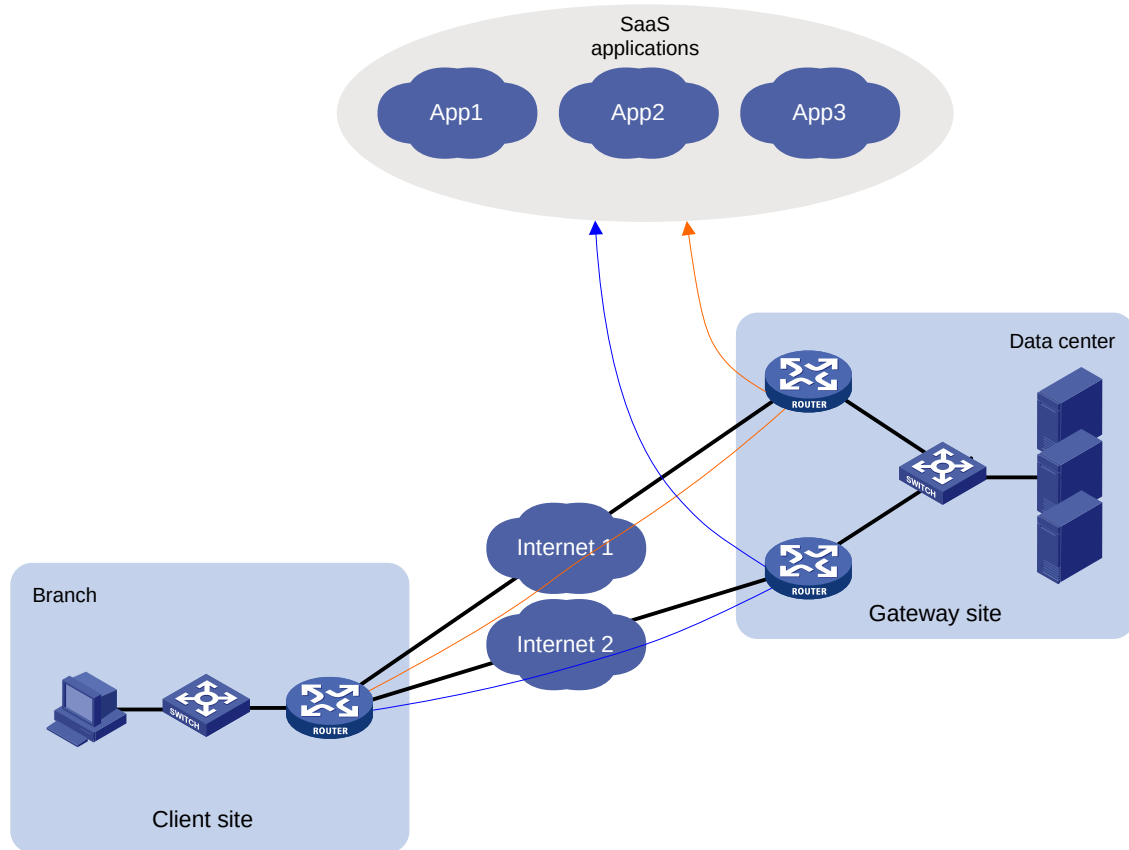
Figure 40 Direct access



Access via a gateway

As shown in Figure 41, the device at the branch site acts as a client and accesses SaaS applications via a gateway. It performs SaaS path optimization based on quality information for the paths that can access SaaS applications via a gateway. This access method is supported only in an RIR-SDWAN network.

Figure 41 Access via a gateway



Hybrid access

The device can directly access SaaS applications without using a gateway and access SaaS applications via a gateway. The device can select optimal paths based on path quality information from both the paths that can directly access SaaS applications and the paths that access SaaS applications via a gateway. This access method is supported only in an RIR-SDWAN network.

SaaS path quality probe

Health check URL

When the device performs path optimization for traffic that accesses a SaaS application, it probes quality for paths that access the SaaS application through the health check URL. Based on the probe results, the device selects an optimal path for the traffic that accesses the SaaS application.

You can specify a health check URL for a user-defined SaaS application.

The health check URL of a predefined SaaS application is defined by the system. You cannot change it.

Probe mechanism

When the device directly accesses SaaS applications or acts as a gateway for other devices to access SaaS applications, it performs path quality probes at intervals of 30 seconds. The device probes quality for paths that can directly access SaaS applications through direct interfaces via the health check URL. Direct interfaces refer to the interfaces that can directly access SaaS applications. Path quality metrics include delay, jitter, and packet loss ratio.

An indirect access path contains an SDWAN tunnel between the client and gateway and a path from the gateway to a SaaS application. The device uses the quality probe mechanisms in RIR-SDWAN to probe the SDWAN tunnel quality. In addition, the device receives path quality information advertised from the gateway for the optimal paths that the gateway uses to access SaaS applications. Based on the information, the device obtains the quality of the indirect access path.

CPEs at the gateway site use BGP IPv4 tunnel-encap-ext routes to advertise SaaS path quality information to an RR. The RR reflects the routes to other CPEs.

SaaS path quality evaluation

CQI

The device computes Comprehensive Quality Indicator (CQI) values to evaluate path quality for a SaaS application.

- If the probe result of a metric (delay, jitter, or packet loss ratio) is lower than or equal to the expected quality value, the CQI value for the metric is 100.
- If the probe result of a metric is higher than the expected quality value, the CQI value for the metric is calculated with the formula: $(\text{expected quality value for the metric} \times 100) / \text{probe result of the metric}$.
- The overall CQI value is calculated with the formula: $(x \times Ds + y \times Js + z \times Ls) / (x + y + z)$.
In this formula, x, y, and z represent the weight values of delay, jitter, and packet loss ratio, respectively (the weight values are in the range of 0 to 10, and cannot be all 0). Ds, Js, and Ls represent the CQI values for delay, jitter, and packet loss ratio.

Quality evaluation mechanism

The device periodically computes the overall CQI value to evaluate quality for paths that can access a SaaS application. When the settings related to CQI computation have changes, for example, quality metric weights or expected quality values are changed, the device also computes the overall CQI value for paths.

- To evaluate quality for a path that can directly access the SaaS application, the device computes the overall CQI value based on the path quality result probed by local interface.
- To evaluate quality for a path that accesses the SaaS application via a gateway, the device uses the average value for the following values as the overall CQI value:
 - The overall CQI value for the path that the gateway uses to directly access the SaaS application. This value is obtained based on the path quality result probed by gateway local interface. The path quality result is advertised to the device through BGP IPv4 tunnel-encap-ext routes.
 - The overall CQI value for the path (SDWAN tunnel) from the device to the gateway. This value is obtained based on the quality probe result for the SDWAN tunnel in RIR-SDWAN.

To avoid frequent link switchovers, the device uses the approximate overall CQI value to evaluate link quality. The approximate overall CQI value is a multiple of 5 that is smaller than and closest to the overall CQI value. For example, if the overall CQI value is 82.5 for paths through which the device indirectly accesses SaaS applications, the approximate overall CQI value is 80.

The device allocates paths to different color areas according to the approximate overall CQI value.

- A path belongs to the green area if its approximate overall CQI value is in the range of 80 to 100.
- A path belongs to the yellow area if its approximate overall CQI value is in the range of 55 to 80.

- A path belongs to the red area if its approximate overall CQI value is in the range of 0 to 50.

CQI-based optimal path selection

The device first selects a color area in the order of green, yellow, and red. Then, it selects an optimal path in the selected color area. If the selected color area has only one path, this path is the optimal path. If the selected color area has multiple paths, the device randomly selects one of the paths as the optimal path.

SaaS path optimization mechanism

Accessing SaaS applications through dynamically allocated IP addresses

Typically, a user uses the URL of a SaaS application to request access to the SaaS application. When the user enters the URL, the endpoint used by the user sends a DNS request for resolving the URL to an IP address. For successful URL resolution, the URL must have been added to the SaaS application instance as an access URL.

When the device receives the DNS request, it performs the following operations for SaaS path optimization:

1. Computes CQI values to evaluate path quality and selects an optimal path based on the CQI values.
2. Forwards the DNS request through the optimal path.
3. Associates the IP address in the received DNS response with the optimal path and adds the association as an optimal path entry.
4. Forwards the DNS response to the user.
5. Upon receiving a packet destined for the IP address in the optimal path entry, the device forwards the packet through the optimal path.

Accessing SaaS applications through static IP addresses

The system defines static IP addresses for predefined SaaS applications. Users can access predefined SaaS applications through the static IP addresses.

When the device receives a service packet destined for a static IP address specified in a predefined SaaS application instance, it examines whether an optimal path entry exists for the static IP address.

- If an optimal path entry exists for the static IP address, the device forwards the packet based on the entry.
- If no optimal path entry exists for the static IP address, the device selects an optimal path based on the quality information for paths that can access the SaaS application. Then, the device forwards the packet through the optimal path, associates the static IP address with the optimal path, and adds the association as an optimal path entry.

Aging for optimal path entries

Optimal path entries will expire after a period of time. The optimal path entries created for dynamic IP addresses will expire 2 minutes after the dynamic IP addresses resolved by DNS expire.

Prerequisites for SaaS path optimization

SaaS path optimization requires resolving DNS packets, so you must enable DNS proxy. For more information about DNS proxy, see DNS in *Layer 3—IP Services Configuration Guide*.

SaaS path optimization tasks at a glance

To configure SaaS path optimization, perform the following tasks:

1. Configuring network parameters for SaaS path optimization

- a. [Creating the SaaS path optimization view](#)
 - b. Specifying a node type for the device
 - c. Specifying an interface for the device to directly access SaaS applications
2. Configuring SaaS application instances
 - a. Creating a SaaS application instance
 - b. Adding access URLs for a SaaS application
 - c. [Configuring the health check URL for a SaaS application](#)
 - d. Configuring the expected quality values for paths accessing a SaaS application
 - e. [Configuring the CQI parameters](#)
 - f. (Optional.) [Matching only packets in the public network or specific VPN instances for SaaS path optimization](#)

Configuring network parameters for SaaS path optimization

Creating the SaaS path optimization view

About this task

To configure SaaS path optimization parameters, you must create the SaaS path optimization view.

Procedure

1. Enter system view.
system-view
2. Create the SaaS path optimization view and enter this view.
saas-path-optimize

Specifying a node type for the device

About this task

Specify a node type for the device according to the method that the device uses to access SaaS applications.

- If the device must use a gateway to access SaaS applications, configure the device as a client without specifying the **allow-direct-access** keyword.
- If the device directly accesses SaaS applications without using a gateway or uses the hybrid method to access SaaS applications, configure the device as a client and specify the **allow-direct-access** keyword.
- If the device directly accesses SaaS applications without using a gateway and acts as a gateway for other devices to access SaaS applications, configure the device as a gateway.

Restrictions and guidelines

If the device uses a gateway to access SaaS applications or uses the hybrid method to access SaaS applications, you must enable RIR-SDWAN on the device. This operation ensures that the device can correctly perform SaaS path optimization.

If the device only accesses SaaS applications directly, you can enable RIR-VXLAN or RIR-SDWAN.

Procedure

1. Enter system view.
system-view

2. Enter SaaS path optimization view.
saas-path-optimize
3. Specify a node type for the device.
node-type { **client** [**allow-direct-access**] | **gateway** }
By default, no node type is specified for the device.

Specifying an interface for the device to directly access SaaS applications

About this task

Perform this task if the device directly accesses SaaS applications or acts as a gateway for other devices to access SaaS applications. After you specify a node type for the device and specify interfaces that can directly access SaaS applications, the device probes path quality at intervals of 30 seconds. The paths are from the specified direct interfaces to SaaS applications. The health check URL in each SaaS application instance is used to access the SaaS applications for path quality probe.

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Specify an interface that can directly access SaaS applications.
direct interface *interface-type interface-number*
By default, no interfaces can directly access SaaS applications.

Configuring SaaS application instances

Creating a SaaS application instance

About this task

To configure path optimization for a SaaS application, you must create a SaaS application instance for that SaaS application.

The system has predefined SaaS application instances. You cannot delete them or add, delete, or change the predefined parameters in them. For example, you cannot add, delete, or change the URLs, health check URL, and static IP addresses in a predefined SaaS application instance.

Restrictions and guidelines

The name of a user-defined SaaS application instance cannot be the same as the name of any existing SaaS application instance (including the name of a predefined SaaS application instance).

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Create a SaaS application instance and enter SaaS application instance view.

application-instance *instance-name*

By default, only predefined SaaS application instances exist.

Adding access URLs for a SaaS application

About this task

Perform this task to add URLs that can be used to access a user-defined SaaS application.

Restrictions and guidelines

This feature is not supported by predefined SaaS applications.

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Enter SaaS application instance view.
application-instance *instance-name*
4. Add an access URL for the SaaS application.
url *url*

By default, no access URLs exist in a user-defined SaaS application instance.

Configuring the health check URL for a SaaS application

About this task

When the device performs path optimization for traffic that accesses a SaaS application, it probes quality for paths that access the SaaS application through the health check URL. Based on the probe results, the device selects an optimal path for the traffic that accesses the SaaS application.

Restrictions and guidelines

This feature is applicable only to user-defined SaaS application instances. The system defines a health check URL for each predefined SaaS application instance. You cannot change the health check URL of a predefined SaaS application instance.

If the health check URL has not been added to a user-defined SaaS application instance, this task automatically adds the URL to the application instance as an access URL.

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Enter SaaS application instance view.
application-instance *instance-name*
4. Configure the health check URL for the SaaS application.
health-url *health-url*

By default, no health check URL is configured a user-defined SaaS application.

Configuring the expected quality values for paths accessing a SaaS application

About this task

When the device performs path optimization for traffic that accesses a SaaS application, it probes quality for the paths that can access the SaaS application. The device calculates CQI values for the paths based on the probe results and the configured expected quality values to evaluate path quality.

Restrictions and guidelines

If the device uses a gateway to access SaaS applications or uses the hybrid method to access SaaS applications, configure the same expected quality values on the client and gateway.

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Enter SaaS application instance view.
application-instance *instance-name*
4. Set the expected delay, jitter, and packet loss ratio for accessing the SaaS application.
expect-quality delay *delay-value* **jitter** *jitter-value* **packet-loss** *packet-loss-ratio*
By default, the expected delay, jitter, and packet loss ratio for accessing a SaaS application are 10 milliseconds, 100 milliseconds, and 100%, respectively.

Configuring the CQI parameters

About this task

The device computes CQI values to evaluate link quality for paths that access a SaaS application. Perform this task to configure the weights for the delay, jitter, and packet loss metrics used for computing CQI values.

Restrictions and guidelines

The weights for the delay, jitter, and packet loss metrics cannot be all 0.

If the device uses a gateway to access SaaS applications or uses the hybrid method to access SaaS applications, configure the same CQI weights on the client and gateway.

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Enter SaaS application instance view.
application-instance *instance-name*
4. Configure the weights for the delay, jitter, and packet loss metrics used for computing CQI values.
cqi-weight delay *delay-weight* **jitter** *jitter-weight* **packet-loss** *packet-loss-weight*
By default, the weights for the delay, jitter, and packet loss metrics are all 1.

Matching only packets in the public network or specific VPN instances for SaaS path optimization

About this task

Perform this task to enable the device to select optimal paths only for packets that access a SaaS application in the public network or specified VPN instances.

Restrictions and guidelines

If you cancel SaaS path optimization for packets that access a SaaS application in the public network and all VPN instances, the device performs SaaS path optimization for all packets that access the SaaS application.

Procedure

1. Enter system view.
system-view
2. Enter SaaS path optimization view.
saas-path-optimize
3. Enter SaaS application instance view.
application-instance *instance-name*
4. Match packets in the public network or a VPN instance for SaaS path optimization.
access-network { **public** | **vpn-instance** *vpn-instance-name* }

By default, the device performs SaaS path optimization for all packets that access a SaaS application.

Command reference

New command: access-network

Use **access-network** to match packets in the public network or a VPN instance for SaaS path optimization.

Use **undo access-network** to cancel SaaS path optimization for packets in the public network or a VPN instance.

Syntax

```
access-network { public | vpn-instance vpn-instance-name }  
undo access-network { public | vpn-instance [ vpn-instance-name ] }
```

Default

The device performs SaaS path optimization for all packets that access a SaaS application.

Views

SaaS application instance view

Predefined user roles

network-admin

Parameters

public: Specifies the public network.

vpn-instance: Specifies VPN instances.

vpn-instance-name: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must already exist.

Usage guidelines

Use this command to enable the device to select optimal paths only for packets that access a SaaS application in the public network or specified VPN instances.

Repeat this command to specify the public network and multiple VPN instances. A SaaS application supports a maximum of eight VPN instances (including the public network) for SaaS path optimization.

If you do not specify a VPN instance for the **undo access-network vpn-instance** [*vpn-instance-name*] command, the command cancels SaaS path optimization for all VPN instances.

If you cancel SaaS path optimization for packets that access a SaaS application in the public network and all VPN instances, the device performs SaaS path optimization for all packets that access the SaaS application.

Examples

Match packets that access SaaS application **App1** in the public network for SaaS path optimization.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] application-instance App1
[Sysname-saas-pathoptimize-App1] access-network public
```

Match packets that access SaaS application **App1** in VPN instance **vpn1** for SaaS path optimization.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] application-instance App1
[Sysname-saas-pathoptimize-App1] access-network vpn-instance vpn1
```

New command: application-instance

Use **application-instance** to create a SaaS application instance and enter its view, or enter the view of an existing SaaS application instance.

Use **undo application-instance** to delete a SaaS application instance.

Syntax

application-instance *instance-name*

undo application-instance *instance-name*

Default

Only predefined SaaS application instances exist.

Views

SaaS path optimization view

Predefined user roles

network-admin

Parameters

instance-name: Specifies a name for the SaaS application instance, a case-sensitive string of 1 to 63 characters. The string cannot contain a backslash (\), quotation mark ("), question mark (?), or space.

Usage guidelines

SaaS applications include predefined SaaS applications and user-defined SaaS applications. Typically, predefined SaaS applications are common SaaS applications. User-defined SaaS applications are manually configured to meet service requirements.

To configure path optimization for a SaaS application, you must create a SaaS application instance for that SaaS application.

The system has predefined SaaS application instances. You cannot delete them or add, delete, or change the predefined parameters in them. For example, you cannot add, delete, or change the URLs, health check URL, and static IP addresses in a predefined SaaS application instance.

Use this command to create a user-defined SaaS application instance and enter its view, or use this command to enter the view of a predefined SaaS application instance.

The name of a user-defined SaaS application instance cannot be the same as the name of any existing SaaS application instance (including the name of a predefined SaaS application instance). To obtain the names of existing SaaS application instances, use the **display saas attribute** command.

The device supports a maximum of 100 user-defined SaaS application instances.

Examples

Create SaaS application instance **App1** and enter its view.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] application-instance App1
[Sysname-saas-pathoptimize-App1]
```

Related commands

display saas attribute

New command: cqi-weight (SaaS application instance view)

Use **cqi-weight** to configure the weights for the delay, jitter, and packet loss metrics used for computing CQI values.

Use **undo cqi-weight** to restore the default.

Syntax

cqi-weight delay *delay-weight* **jitter** *jitter-weight* **packet-loss** *packet-loss-weight*
undo cqi-weight

Default

The weights for the delay, jitter, and packet loss metrics are all 1.

Views

SaaS application instance view

Predefined user roles

network-admin

Parameters

delay *delay-weight*: Sets the weight for the delay metric used for computing CQI values, in the range of 0 to 10.

jitter *jitter-weight*: Sets the weight for the jitter metric used for computing CQI values, in the range of 0 to 10.

packet-loss *packet-loss-weight*: Sets the weight for the packet loss metric used for computing CQI values, in the range of 0 to 10.

Usage guidelines

The device computes Comprehensive Quality Indicator (CQI) values to evaluate path quality for a SaaS application.

- If the probe result of a metric (delay, jitter, or packet loss ratio) is lower than or equal to the expected quality value, the CQI value for the metric is 100.
- If the probe result of a metric is higher than the expected quality value, the CQI value for the metric is calculated with the formula: (expected quality value for the metric × 100) / probe result of the metric.
- The overall CQI value is calculated with the formula: $(x \times Ds + y \times Js + z \times Ls) / (x + y + z)$.

In this formula, x, y, and z represent the weight values of delay, jitter, and packet loss ratio, respectively. Ds, Js, and Ls represent the CQI values for delay, jitter, and packet loss ratio.

To evaluate quality for a path that can directly access the SaaS application, the device computes the overall CQI value based on the path quality result probed by local interface.

To evaluate quality for a path that accesses the SaaS application via a gateway, the device uses the average value for the following values as the overall CQI value:

- The overall CQI value for the path that the gateway uses to directly access the SaaS application. This value is obtained based on the path quality result probed by gateway local interface. The path quality result is advertised to the device through BGP IPv4 tunnel-encap-ext routes.
- The overall CQI value for the path (SDWAN tunnel) from the device to the gateway. This value is obtained based on the quality probe result for the SDWAN tunnel in RIR-SDWAN.

To avoid frequent link switchovers, the device uses the approximate overall CQI value to evaluate link quality. The approximate overall CQI value is a multiple of 5 that is smaller than and closest to the overall CQI value. For example, if the overall CQI value is 82.5 for paths through which the device indirectly accesses SaaS applications, the approximate overall CQI value is 80.

The device allocates paths to different color areas according to the approximate overall CQI value.

- A path belongs to the green area if its approximate overall CQI value is in the range of 80 to 100.
- A path belongs to the yellow area if its approximate overall CQI value is in the range of 55 to 80.
- A path belongs to the red area if its approximate overall CQI value is in the range of 0 to 50.

The device first selects a color area in the order of green, yellow, and red. Then, it selects an optimal path in the selected color area. If the selected color area has only one path, this path is the optimal path. If the selected color area has multiple paths, the device randomly selects one of the paths as the optimal path.

The weights for the delay, jitter, and packet loss metrics cannot be all 0.

Examples

In SaaS application instance **App1**, configure the weight values for the delay, jitter, and packet loss metrics as 2, 5, and 7, respectively, to compute CQI values for path quality evaluation.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] application-instance App1
[Sysname-saas-pathoptimize-App1] cqi-weight delay 2 jitter 5 packet-loss 7
```

Related commands

expect-quality

New command: direct interface

Use **direct interface** to specify an interface for the device to directly access SaaS applications.

Use **undo direct interface** to disable the device from using specific interfaces to directly access SaaS applications.

Syntax

direct interface *interface-type interface-number*

undo direct interface [*interface-type interface-number*]

Default

No interfaces are specified for the device to directly access SaaS applications.

Views

SaaS path optimization view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface for the **undo direct interface** command, the command disable the device from using all interfaces to directly access SaaS applications.

Usage guidelines

Use this command if the device directly accesses SaaS applications or acts as a gateway for other devices to access SaaS applications. After you use the **node-type** command to specify a node type and use the **direct interface** command to specify interfaces, the device probes path quality at intervals of 30 seconds. The paths are from the specified direct interfaces to SaaS applications. The health check URL in each SaaS application instance is used to access the SaaS applications for path quality probe.

The device supports a maximum of 10 interfaces through which the device can directly access SaaS applications.

Examples

```
# Allow the device to directly access SaaS applications through interface GigabitEthernet 1/0/2.
```

```
<Sysname> system-view
```

```
[Sysname] saas-path-optimize
```

```
[Sysname-saas-pathoptimize] direct interface gigabitethernet 1/0/2
```

New command: display saas attribute

Use **display saas attribute** to display attribute information for SaaS applications.

Syntax

display saas attribute [**verbose** [**application-instance** *instance-name*]]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

verbose: Displays detailed attribute information for SaaS applications. If you do not specify this keyword, the command displays only brief attribute information for SaaS applications.

application-instance *instance-name*: Specifies a SaaS application instance by its name, a case-sensitive string of 1 to 63 characters. The string cannot contain a backslash (\), quotation mark ("), question mark (?), or space. If you do not specify this option following the **verbose** keyword, the command displays detailed attribute information for all predefined and user-defined SaaS applications.

Examples

Display detailed attribute information for all predefined and user-defined SaaS applications.

```
<Sysname> display saas attribute verbose

SaaS application      : Appl
Health check URL     : www.applurl1.com
URL list              : www.applurl1.com
                       www.applurl2.com
                       www.applurl3.com
                       www.applurl4.com
Static IP address     : 10.124.25.36
                       10.124.25.37

SaaS application      : office365
Health check URL     : www.office.com
URL list              : *.broadcast.skype.com
                       *.lync.com
                       *.mail.protection.outlook.com
                       *.manage.office.com
                       *.msapproxy.net
                       *.msftidentity.com
                       *.msidentity.com
                       *.online.office.com
                       *.outlook.office.com
                       *.portal.cloudappsecurity.com
                       *.protection.office.com
                       *.protection.outlook.com
                       *.sharepoint.com
                       *.skypeforbusiness.com
                       *.teams.microsoft.com
                       *.broadcast.officeapps.live.com
                       *.excel.officeapps.live.com
                       *.onenote.officeapps.live.com
                       *.powerpoint.officeapps.live.com
                       *.rtc.officeapps.live.com
                       *.shared.officeapps.live.com
                       *.view.officeapps.live.com
```

*visio.officeapps.live.com
 *word-edit.officeapps.live.com
 account.activedirectory.windowsazure.com
 account.office.net
 accounts.accesscontrol.windows.net
 admin.microsoft.com
 adminwebservice.microsoftonline.com
 api.passwordreset.microsoftonline.com
 autologon.microsoftazuread-sso.com
 becws.microsoftonline.com
 broadcast.skype.com
 clientconfig.microsoftonline-p.net
 companymanager.microsoftonline.com
 device.login.microsoftonline.com
 graph.microsoft.com
 graph.windows.net
 home.office.com
 login-us.microsoftonline.com
 login.microsoft.com
 login.microsoftonline-p.com
 login.microsoftonline.com
 login.windows.net
 logincert.microsoftonline.com
 loginex.microsoftonline.com
 manage.office.com
 nexus.microsoftonline-p.com
 nexus.officeapps.live.com
 nexusrules.officeapps.live.com
 office.live.com
 outlook.office.com
 outlook.office365.com
 passwordreset.microsoftonline.com
 portal.microsoftonline.com
 portal.office.com
 protection.office.com
 provisioningapi.microsoftonline.com
 smtp.office365.com
 teams.microsoft.com
 www.office.com

Static IP address : 13.80.125.22
 13.91.91.243
 13.107.6.152
 13.107.6.156
 13.107.6.171
 13.107.7.190
 13.107.9.156
 13.107.18.10
 13.107.64.0

```

13.107.128.0
13.107.136.0
13.107.140.6
20.190.128.0
23.103.160.0
40.81.156.154
40.90.218.198
40.92.0.0
40.96.0.0
40.104.0.0
40.107.0.0
40.108.128.0
40.126.0.0
52.96.0.0
52.100.0.0
52.104.0.0
52.108.0.0
52.112.0.0
52.120.0.0
52.174.56.180
52.183.75.62
52.184.165.82
52.238.78.88
52.238.106.116
52.238.119.141
52.244.37.168
52.244.160.207
52.244.203.72
52.244.207.172
52.244.223.198
52.247.150.191
104.42.230.91
104.47.0.0
104.146.128.0
131.253.33.215
132.245.0.0
150.171.32.0
150.171.40.0
157.55.145.0
157.55.155.0
157.55.227.192
204.79.197.215

```

Display brief attribute information for all predefined and user-defined SaaS applications.

```
<Sysname> display saas attribute
```

SaaS application	IsCustomize
App1	NO
office365	Yes

Table 68 Command output

Field	Description
SaaS application	SaaS application name.
URL list	URLs used to access the SaaS application.
Static IP addresses	Static IP addresses used to access a predefined SaaS application. If no static IP addresses exist, this field displays a hyphen (-).
IsCustomized	Whether the SaaS application is a predefined SaaS application. Yes—Predefined SaaS application. No—User-defined SaaS application.

New command: display saas optimal-path

Use **display saas optimal-path** to display information for optimal paths that can access a SaaS application.

Syntax

display saas optimal-path application-instance *instance-name*

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

application-instance *instance-name*: Specifies a SaaS application instance by its name, a case-sensitive string of 1 to 63 characters. The string cannot contain a backslash (\), quotation mark ("), question mark (?), or space.

Examples

Display information for optimal paths that can access SaaS application **App1**.

```
<Sysname> display saas optimal-path application-instance App1
SaaS application: App1
```

UserIP	DirectInterface	TunnelID	SiteID	DevID	IfID
10.125.36.33	GE1/0/1	-	-	-	-
10.125.27.45	-	1	30	2	2

Table 69 Command output

Field	Description
SaaS application	SaaS application name.
UserIP	IP address used by a user to access the SaaS application.
DirectInterface	Name of an interface through which the device can directly access the SaaS application.
TunnelID	SDWAN tunnel ID.

Field	Description
SiteID	Gateway site ID.
DevID	Gateway device ID.
IfID	Interface ID of the peer TTE for the SDWAN tunnel.

New command: display saas path-cqi

Use **display saas path-cqi** to display CQI information for paths that can access SaaS applications.

Syntax

display saas path-cqi [**application-instance** *instance-name*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

application-instance *instance-name*: Specifies a SaaS application instance by its name, a case-sensitive string of 1 to 63 characters. The string cannot contain a backslash (\), quotation mark ("), question mark (?), or space. If you do not specify a SaaS application instance, this command displays CQI information for all paths that can access predefined and user-defined SaaS applications.

Examples

Display CQI information for paths that can access SaaS application **App1**.

```
<Sysname> display saas path-cqi application-instance App1
SaaS application: App1
```

DirectInterface	TunnelID	SiteID	DevID	IfID	CQI	Color
GE1/0/1	-	-	-	-	90	Green
-	1	9	2	2	85	Green
GE1/0/3	-	-	-	-	80	Yellow
GE1/0/2	-	-	-	-	75	Yellow
GE1/0/4	-	-	-	-	65	Yellow
-	1	9	5	4	50	Red
GE1/0/6	-	-	-	-	45	Red

Table 70 Command output

Field	Description
SaaS application	SaaS application name.
DirectInterface	Name of an interface through which the device can directly access the SaaS application.
TunnelID	SDWAN tunnel ID.
SiteID	Gateway site ID.

Field	Description
DevID	Gateway device ID.
IfID	Interface ID of the peer TTE for the SDWAN tunnel.
CQI	Approximate overall CQI value for the path.
Color	Color area to which the path belongs.

New command: display saas path-quality

Use **display saas path-quality** to display quality information for paths that can access SaaS applications.

Syntax

```
display saas path-quality { client-to-gateway | gateway-to-saas | local-to-saas }
[ application-instance instance-name ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

client-to-gateway: Displays quality information for the SDWAN tunnels from the client to the gateway. Do not specify this keyword if the device only accesses SaaS applications directly or the device acts as a gateway for other devices to access SaaS applications.

gateway-to-saas: Displays quality information for the optimal paths from the gateway to SaaS applications. Do not specify this keyword if the device only accesses SaaS applications directly or the device acts as a gateway for other devices to access SaaS applications.

local-to-saas: Displays quality information for the paths from the local device to SaaS applications. Do not specify this keyword if the device accesses SaaS applications only via a gateway.

application-instance *instance-name*: Specifies a SaaS application instance by its name, a case-sensitive string of 1 to 63 characters. The string cannot contain a backslash (\), quotation mark ("), question mark (?), or space. If you do not specify a SaaS application instance, this command displays quality information for all paths that can access predefined and user-defined SaaS applications.

Examples

Display quality information for the paths from the local device to SaaS applications.

```
<Sysname> display saas path-quality local-to-saas
SaaS application: Appl
```

DirectInterface	PktLoss(per mill)	Delay(ms)	Jitter(ms)	CQI
-----	-----	-----	-----	-----
GE1/0/1	50	20	3	80
GE1/0/2	45	30	5	85
GE1/0/3	55	20	4	85
GE1/0/4	57	10	5	90
GE1/0/5	80	10	3	80

GE1/0/6	80	20	2	85

SaaS application: App2

DirectInterface	PktLoss(per mill)	Delay(ms)	Jitter(ms)	CQI
GE1/0/1	50	10	3	80
GE1/0/2	45	20	5	85
GE1/0/3	55	25	4	85
GE1/0/4	57	15	5	90
GE1/0/5	80	10	3	80
GE1/0/6	90	30	1	85

Display quality information for the optimal paths from the gateway to SaaS applications.

<Sysname> display saas path-quality gateway-to-saas

SaaS application: App1

SiteID	DevID	GatewayIP	PktLoss(per mill)	Delay(ms)	Jitter(ms)	CQI
10	5	1.1.1.1	50	20	4	80
20	4	2.2.2.2	40	25	3	85
10	4	3.3.3.3	30	15	2	90

SaaS application: App2

SiteID	DevID	GatewayIP	PktLoss(per mill)	Delay(ms)	Jitter(ms)	CQI
10	5	1.1.1.1	40	20	5	85
20	4	2.2.2.2	50	20	2	80
10	4	3.3.3.3	35	25	4	90

Display quality information for the SDWAN tunnels from the client to the gateway.

<Sysname> display saas path-quality client-to-gateway

SaaS application: App1

GatewayInfo: SiteID=10 DevID=5 GatewayIP=1.1.1.1

TunnelID	IfID	PktLoss(per mill)	Delay(ms)	Jitter(ms)	CQI
1	2	50	20	3	85
1	3	40	30	4	80
1	4	60	30	2	90
1	5	50	25	5	75

GatewayInfo: SiteID=20 DevID=4 GatewayIP=2.2.2.2

TunnelID	IfID	PktLoss(per mill)	Delay(ms)	Jitter(ms)	CQI
2	2	45	30	4	90
2	3	50	20	3	70

2	4	65	25	2	85
2	5	40	30	4	90

SaaS application: App2

GatewayInfo: SiteID=10 DevID=5 GatewayIP=1.1.1.1

TunnelID	IfID	PktLoss (per mill)	Delay (ms)	Jitter (ms)	CQI
4	2	45	10	3	80
4	3	50	20	3	85
4	4	55	25	4	95
4	5	45	10	6	70

GatewayInfo: SiteID=20 DevID=4 GatewayIP=2.2.2.2

TunnelID	IfID	PktLoss (per mill)	Delay (ms)	Jitter (ms)	CQI
4	2	40	20	4	85
4	3	30	10	5	95
4	4	30	10	3	85
4	5	50	15	6	75

Table 71 Command output

Field	Description
SaaS application	SaaS application name.
DirectInterface	Name of an interface through which the device can directly access the SaaS application.
PktLoss	Packet loss ratio per mille.
Delay	Path delay, in milliseconds.
Jitter	Path jitter, in milliseconds.
CQI	Approximate overall CQI value for the path.
GatewayInfo	Gateway information.
SiteID	Gateway site ID.
DevID	Gateway device ID.
GatewayIP	Gateway IP address. A gateway IP address uniquely identifies a gateway.
TunnelID	SDWAN tunnel ID.
IfID	Interface ID of the peer TTE for the SDWAN tunnel.

New command: expect-quality

Use **expect-quality** to set the expected delay, jitter, and packet loss ratio for accessing a SaaS application.

Use **undo expect-quality** to restore the default.

Syntax

expect-quality delay *delay-value* **jitter** *jitter-value* **packet-loss** *packet-loss-ratio*
undo expect-quality

Default

The expected delay, jitter, and packet loss ratio for accessing a SaaS application are 10 milliseconds, 100 milliseconds, and 100‰, respectively.

Views

SaaS application instance view

Predefined user roles

network-admin

Parameters

delay *delay-value*: Sets the expected delay, in the range of 0 to 3600000 milliseconds.

jitter *jitter-value*: Sets the expected jitter, in the range of 10 to 60000 milliseconds.

packet-loss *packet-loss-ratio*: Specifies the expected packet loss ratio, in the range of 0 to 1000 per mille.

Usage guidelines

When the device performs path optimization for traffic that accesses a SaaS application, it probes quality for the paths that can access the SaaS application. The device calculates CQI values for the paths based on the probe results and the configured expected quality values to evaluate path quality.

Examples

Set the expected delay, jitter, and packet loss ratio for accessing SaaS application **App1** to 1000 milliseconds, 1000 milliseconds, and 500‰, respectively.

```
<Sysname> system-view
```

```
[Sysname] saas-path-optimize
```

```
[Sysname-saas-pathoptimize] application-instance App1
```

```
[Sysname-saas-pathoptimize-App1] expect-quality delay 1000 jitter 1000 packet-loss 500
```

Related commands

cqi-weight (SaaS application instance view)

New command: health-url

Use **health-url** to configure the health check URL for a SaaS application.

Use **undo health-url** to restore the default.

Syntax

health-url *health-url*

undo health-url

Default

No health check URL is configured for a SaaS application.

Views

SaaS application instance view

Predefined user roles

network-admin

Parameters

health-url: Specifies a URL as the health check URL. The URL is a case-insensitive string of 1 to 63 characters. The string cannot contain a back slash (\), quotation mark, question mark (?), or space. If the string contains an asterisk (*), the asterisk (*) must be the first character.

Usage guidelines

When the device performs path optimization for traffic that accesses a SaaS application, it probes quality for paths that access the SaaS application through the health check URL. Based on the probe results, the device selects an optimal path for the traffic that accesses the SaaS application.

This command is applicable only to user-defined SaaS application instances. The system defines a health check URL for each predefined SaaS application instance. You cannot change the health check URL of a predefined SaaS application instance.

If the health check URL has not been added to a user-defined SaaS application instance, this command automatically adds the URL to the application instance as an access URL.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the health check URL as www.app1url1.com for user-defined SaaS application **App1**.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] application-instance App1
[Sysname-saas-pathoptimize-App1] health-url www.app1url1.com
```

Related commands

url

New command: node-type

Use **node-type** to specify a node type for the device.

Use **undo node-type** to restore the default.

Syntax

node-type { **client** [**allow-direct-access**] | **gateway** }

undo node-type

Default

No node type is specified for the device.

Views

SaaS path optimization view

Predefined user roles

network-admin

Parameters

client: Configures the device as a client.

allow-direct-access: Allows the device to directly access SaaS applications through local interfaces. If you do not specify this keyword following the **client** keyword, the device acts only as a client and it must access SaaS applications via a gateway.

gateway: Configures the device as a gateway.

Usage guidelines

The device can use one of the following methods to access SaaS applications:

- **Direct access**—The device directly accesses SaaS applications through local interfaces and performs SaaS path optimization based on local quality information for the paths that can directly access SaaS applications.
- **Access via a gateway**—The device acts as a client and accesses SaaS applications via a gateway. For high availability, deploy multiple gateways. The device performs SaaS path optimization based on quality information for the paths that can access SaaS applications via a gateway. An indirect access path contains an SDWAN tunnel between the client and gateway and a path from the gateway to a SaaS application. The device uses the quality probe mechanisms in RIR-SDWAN to probe the SDWAN tunnel quality. In addition, the device receives path quality information advertised from the gateway for the optimal paths that the gateway uses to access SaaS applications. Based on the information, the device obtains the quality of the indirect access path.

CPEs at the gateway site use BGP IPv4 tunnel-encap-ext routes to advertise SaaS path quality information to an RR. The RR reflects the routes to other CPEs.

- **Hybrid access**—The device can directly access SaaS applications without using a gateway and access SaaS applications via a gateway. The device can select optimal paths based on path quality information from both the paths that can directly access SaaS applications and the paths that access SaaS applications via a gateway.

Specify a node type for the device according to the method that the device uses to access SaaS applications.

- If the device must use a gateway to access SaaS applications, configure the device as a client without specifying the **allow-direct-access** keyword.
- If the device directly accesses SaaS applications without using a gateway or uses the hybrid method to access SaaS applications, configure the device as a client and specify the **allow-direct-access** keyword.
- If the device directly accesses SaaS applications without using a gateway and acts as a gateway for other devices to access SaaS applications, configure the device as a gateway.

If the device uses a gateway to access SaaS applications or uses the hybrid method to access SaaS applications, you must enable RIR-SDWAN on the device. This operation ensures that the device can correctly perform SaaS path optimization.

If the device only accesses SaaS applications directly without using a gateway, you can enable RIR-VXLAN or RIR-SDWAN.

Examples

```
# Configure the device as a client and allow the client to directly access SaaS applications through local interfaces.
```

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] node-type client allow-direct-access
```

New command: saas-path-optimize

Use **saas-path-optimize** to create the SaaS path optimization view.

Use **undo saas-path-optimize** to delete the SaaS path optimization view and all settings in the view.

Syntax

saas-path-optimize

undo saas-path-optimize

Default

The SaaS path optimization view does not exist.

Views

System view

Predefined user roles

network-admin

Usage guidelines

SaaS path optimization enables the device to select optimal paths for traffic that accesses SaaS applications and adjust the optimal paths accordingly when path quality changes. In SaaS path optimization view, you can configuration parameters for SaaS path optimization.

If the RIR process is not enabled on the device, executing this command also enables the RIR process. Executing the **undo** form of the command does not disable the RIR process.

To disable the RIR-VXLAN or RIR-SDWAN service, you must first use the **undo saas-path-optimize** command to delete the SaaS path optimization view.

Examples

Enter SaaS path optimization view.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize]
```

Related commands

rir

rir sdwan

New command: url

Use **url** to add URLs that can be used to access a user-defined SaaS application.

Use **undo url** to delete URLs that can be used to access a user-defined SaaS application.

Syntax

url *url*

undo url [*url*]

Default

No access URLs exist in a user-defined SaaS application instance.

Views

SaaS application instance view

Predefined user roles

network-admin

Parameters

url: Specifies a URL for accessing the SaaS application, a case-insensitive string of 1 to 63 characters. The string cannot contain a back slash (\), quotation mark ("), question mark (?), or space. If you do not specify a URL for the **undo url** command, the command deletes all URLs in the SaaS application instance except the health check URL.

Usage guidelines

This command is not supported by predefined SaaS applications. The access URLs of predefined SaaS applications are defined by the system. You cannot add, delete, or change access URLs for predefined SaaS applications.

When the device performs path optimization for traffic that accesses a SaaS application, it probes quality for paths that access the SaaS application through the health check URL. When the device receives a DNS request that contains a URL for accessing the SaaS application, it performs the following operations for SaaS path optimization:

1. Selects an optimal path based on the path quality information obtained by probing the health check URL.
2. Forwards the DNS request through the optimal path.
3. Associates the IP address in the received DNS response with the optimal path and adds the association as an optimal path entry.
4. Forwards the DNS response to the user.
5. Upon receiving a packet destined for the IP address in the optimal path entry, the device forwards the packet through the optimal path.

Users can access predefined SaaS applications through static IP addresses. When the device receives a service packet destined for a static IP address specified in a predefined SaaS application instance, it examines whether an optimal path entry exists for the static IP address.

- If an optimal path entry exists for the static IP address, the device forwards the packet based on the entry.
- If no optimal path entry exists for the static IP address, the device selects an optimal path based on the quality information for paths that can access the SaaS application. Then, the device forwards the packet through the optimal path, associates the static IP address with the optimal path, and adds the association as an optimal path entry.

A URL can be added only to one SaaS application instance.

The **undo url** command cannot delete the health check URL.

You can add a maximum of 100 URLs to a user-defined SaaS application instance.

Examples

Add URL www.app1url1.com for accessing SaaS application **App1**.

```
<Sysname> system-view
[Sysname] saas-path-optimize
[Sysname-saas-pathoptimize] application-instance App1
[Sysname-saas-pathoptimize-App1] url www.app1url1.com
```

Related commands

health-url

New feature: Specifying a VXLAN tunnel as a dedicated link for a flow template

Specifying a VXLAN tunnel as a dedicated link for a flow template

About this task

This task is applicable when you want to forward only specific service flows through a tunnel, for example, to forward video conference traffic through a VXLAN tunnel created based on MPLS VPN.

RIR preferentially selects the dedicated links for the service flows in the specified flow template as follows:

- If only one dedicated link is available, RIR selects the link for forwarding.
- If multiple dedicated links are available, RIR selects a link with the highest preference as specified in the **path link-type index preference** command. If multiple dedicated links with the same preference are available, RIR load shares traffic among the dedicated links based on the link load balancing mode configured for the flow template.
- If no dedicated links are available, RIR selects optimal links from the flow template.

When selecting the dedicated links, the device schedules existing service flows from the dedicated links to other links. If the scheduling fails, the device drops the service flows to ensure traffic stability on the dedicated links. When the dedicated links are no longer used, the device schedules the previous service flows back to the dedicated links.

Restrictions and guidelines

You must specify the dedicated links for the flow template of the target service flows. Without the configuration, the device will not use the links as dedicated links for the service flows.

You can specify a tunnel as the dedicated link for only one service flow, and specify multiple dedicated links for the same service flow.

Procedure

1. Enter system view.
system-view
2. Enter VXLAN tunnel interface view.
interface tunnel *tunnel-number* mode vxlan
3. Specify the VXLAN tunnel as a dedicated link for a flow template.
rir dedicated flow *flow-id*

By default, a VXLAN tunnel is not a dedicated link for a flow template.

Command reference

New command: rir dedicated flow

Use **rir dedicated flow** to specify a VXLAN tunnel as a dedicated link for a flow template.

Use **undo rir dedicated flow** to restore the default.

Syntax

rir dedicated flow *flow-id*

undo rir dedicated flow *flow-id*

Default

A VXLAN tunnel is not a dedicated link for a flow template.

Views

VXLAN tunnel interface view

Predefined user roles

network-admin

Parameters

flow-id: Specifies a flow ID for the flow template. The flow ID is in the range of 1 to 65535.

Usage guidelines

If the RIR process is not enabled on the device, executing this command also enables the RIR process. Executing the **undo** form of the command does not disable the RIR process.

This command is applicable when you want to forward only specific service flows through a tunnel, for example, to forward video conference traffic through a VXLAN tunnel created based on MPLS VPN.

RIR preferentially selects the dedicated links for the service flows in the specified flow template as follows:

- If only one dedicated link is available, RIR selects the link for forwarding.
- If multiple dedicated links are available, RIR selects a link with the highest preference as specified in the **path link-type index preference** command. If multiple dedicated links with the same preference are available, RIR load shares traffic among the dedicated links based on the link load balancing mode configured for the flow template.
- If no dedicated links are available, RIR selects optimal links from the flow template.

When selecting the dedicated links, the device schedules existing service flows from the dedicated links to other links. If the scheduling fails, the device drops the service flows to ensure traffic stability on the dedicated links. When the dedicated links are no longer used, the device schedules the previous service flows back to the dedicated links.

After configuring this command, execute the **path link-type index preference** command for the flow template to configure the preferences for the dedicated links. Without the preference settings, the device will not use the links as dedicated links for service flows.

You can specify a tunnel as the dedicated link for only one service flow, and specify multiple dedicated links for the same service flow.

Examples

Specify Tunnel 1 as the dedicated link for flow template 1.

```
<Sysname> system-view
[Sysname] interface tunnel 1 mode vxlan
[Sysname-Tunnel1] rir dedicated flow 1
```

Related commands

path link-type index preference

New feature: Enabling the device to drop service flows upon failure to find an optimal link

Enabling the device to drop service flows upon failure to find an optimal link

About this task

The device can use RIR to select optimal links to forward service flows of a flow template. If the device fails to find an optimal link, it forwards the service flows according to routing table lookup. If all links specified for a service fail, you can perform this task to avoid use of other links, for example, to prevent lower-priority video traffic to occupy service links.

Procedure

1. Enter system view.
system-view
2. Enter RIR view.
rir
3. Enter flow template view.
flow *flow-id*
4. Enable the device to drop service flows upon failure to find an optimal link.
no-optimal-link drop

By default, upon failure to find an optimal link, the device forwards the service flows according to routing table lookup.

Command reference

New command: no-optimal-link drop

no-optimal-link drop

Use **no-optimal-link drop** to enable the device to drop service flows upon failure to find an optimal link.

Use **undo no-optimal-link drop** to restore the default.

Syntax

no-optimal-link drop

undo no-optimal-link drop

Default

If the device fails to find an optimal link, it forwards the service flows according to routing table lookup.

Views

Flow template view

Predefined user roles

network-admin

Usage guidelines

The device can use RIR to select optimal links to forward service flows of a flow template. If the device fails to find an optimal link, it forwards the service flows according to routing table lookup. If all links specified for a service fail, you can execute this command to avoid use of other links, for example, to prevent lower-priority video traffic to occupy service links.

Examples

Enable the device to drop service flows in flow template 1 upon failure to find an optimal link.

```
<Sysname> system-view
[Sysname] rir
[Sysname-rir] flow 1
[Sysname-rir-flow-1] no-optimal-link drop
```


Related commands

path link-type index preference

New feature: Configuring FEC optimization parameters

Configuring FEC optimization parameters

About this task

You can tune the following FEC optimization parameters for better audio and video quality according to the packet loss and traffic rate on your network.

Procedure

1. Enter system view.
system-view
2. Create a WAAS policy and enter WAAS policy view.
waas policy *policy-name*
By default, a predefined WAAS policy named **waas_default** exists.
3. Specify a class or an RTP WAAS class and enter WAAS policy class view or WAAS policy RTP class view.
 - o **class *class-name* [*insert-before existing-class*]**
By default, no WAAS class is specified.
 - o **rtp-class *class-name* [*insert-before existing_class*]**
By default, no RTP WAAS class is specified.
4. Specify an FEC type.
fec loss-recovery-type { *adaptive-fec* | *determined-fec* }
The default is **determined-fec**.
5. (Optional.) Set the aging time for decoder information.
fec probe aging-time *seconds*
The default setting is 1 second.
This command is supported only for A-FEC.
6. (Optional.) Set the sampling interval.
fec sample-interval *interval*
The default setting is 100 milliseconds.
This command is supported only for A-FEC.

Command reference

fec loss-recovery-type

Use **fec loss-recovery-type** to specify the FEC type.

Use **undo fec loss-recovery-type** to restore the default.

Syntax

```
fec loss-recovery-type { adaptive-fec | determined-fec }  
undo fec loss-recovery-type
```

Default

The FEC type is D-FEC.

Views

WAAS policy class view
WAAS policy RTP class view

Predefined user roles

network-admin

Parameters

adaptive-fec: Specifies adaptive FEC (A-FEC).
determined-fec: Specifies determined FEC (D-FEC).

Usage guidelines

If the FEC average ratio is set to a greater value, more bandwidth will be consumed. If the FEC average ratio is set to a small value, lost packets cannot be recovered. A-FEC adjusts the FEC average ratio based on the calculated real-time packet loss ratio. The adjusted FEC average ratio will not be greater than the set FEC average ratio. D-FEC always uses the set FEC average ratio.

Examples

```
# Set the FEC type to A-FEC.  
<Sysname> system-view  
[Sysname] waas policy waas_rtp  
[Sysname-waaspolicy-waas_rtp] rtp-class rtpclass1  
[Sysname-waaspolicy-waas_rtp-rtpclass1] fec loss-recovery-type adaptive-fec
```

fec probe aging-time

Use **fec probe aging-time** to set the aging time for A-FEC decoder information.
Use **undo fec probe aging-time** to restore the default.

Syntax

```
fec probe aging-time seconds  
undo fec probe aging-time
```

Default

The aging time for A-FEC decoder information is 1 second.

Views

WAAS policy class view
WAAS policy RTP class view

Predefined user roles

network-admin

Parameters

seconds: Specifies the aging time in the range of 0 to 60 seconds.

Usage guidelines

If the encoder receives sampled packets within the aging time, it adjusts the FEC average ratio based on the real-time packet loss ratio. If the encoder does not receive sampled packets within the aging time, it deletes the local decoder information and uses the set FEC average ratio.

Setting the aging time to 0 disables aging.

Examples

Set the aging time for A-FEC decoder information to 5 seconds.

```
<Sysname> system-view
[Sysname] waas policy waas_rtp
[Sysname-waaspolicy-waas_rtp] rtp-class rtpclass1
[Sysname-waaspolicy-waas_rtp-rtpclass1] fec probe aging-time 5
```

fec sample-interval

Use **fec sample-interval** to set the A-FEC sampling interval.

Use **undo fec sample-interval** to restore the default.

Syntax

fec sample-interval *interval*

undo fec sample-interval

Default

The A-FEC sampling interval is 100 milliseconds.

Views

WAAS policy class view

WAAS policy RTP class view

Predefined user roles

network-admin

Parameters

interval: Specifies the A-FEC sampling interval in the range of 1 to 1000 milliseconds.

Usage guidelines

The decoder regularly sends sampled packets to notify the encoder of the real-time packet loss ratio. The encoder adjusts the FEC average ratio based on the real-time packet loss ratio.

Examples

Set the aging time for A-FEC decoder information to 50 milliseconds.

```
<Sysname> system-view
[Sysname] waas policy waas_rtp
[Sysname-waaspolicy-waas_rtp] rtp-class rtpclass1
[Sysname-waaspolicy-waas_rtp-rtpclass1] fec sample-interval 50
```

New feature: Specifying the 5G NR network mode for the 5G modem to register with

Specifying the 5G NR network mode for the 5G modem to register with

1. Enter system view.
system-view
2. Enter cellular interface view.
controller cellular *interface-number*
3. Specify the 5G NR network mode for the 5G modem to register with.
nr mode { nsa | sa | auto }

By default, a 5G modem registers with a 5G NR network deployed in SA mode preferentially than that deployed in NSA mode.

Command reference

nr mode

Use **nr mode** to specify the 5G NR network mode for the 5G modem to register with.

Use **undo nr mode** to restore the default.

Syntax

nr mode { nsa | sa | auto }

undo nr mode

Default

A 5G modem registers with a 5G NR network deployed in SA mode preferentially than that deployed in NSA mode.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

nsa: Specifies the 5G NR network in NSA mode for the 5G modem to register with.

sa: Specifies the 5G NR network in SA mode for the 5G modem to register with.

auto: Enables the 5G modem to register with a 5G NR network deployed in SA mode preferentially than that deployed in NSA mode.

Examples

Specify the 5G network in NSA mode for the 5G modem to register with.

```
<Sysname> system-view
[Sysname] controller cellular 0/0
[Sysname-Cellular0/0]nr mode nsa
Related commands
nr band
```

New feature: Configuring TCP packet compression or decompression

Configuring TCP packet compression or decompression

About this task

You configure TCP packet compression on the upstream device and configure TCP packet decompression on the downstream device. The upstream device compresses packets and forwards them to the downstream device. The downstream device decompresses the received packets and then forwards them.

Restrictions and guidelines

Fragmented packets and packets with the Options field are not compressed or decompressed.

You can enable TCP packet compression or decompression for the same destination IP address, but not both.

Procedure

1. Enter system view.
system-view
2. Enable TCP packet compression or decompression.
waas tcp { compress [max *max-number*] | decompress }
By default, TCP packet compression and decompression is disabled.
3. Specify the destination IP address and destination port number of TCP packets to be compressed or decompressed.
waas tcp destination { ip-address port *port-number* | object-group *ip-object-group-name* port object-group port-object-group-name }
By default, no destination IP address and destination port number are specified.

Command reference

display waas statistics tcp compress

Use **display waas statistics tcp compress** to display TCP packet compression statistics.

Syntax

display waas statistics tcp compress

Views

Any view

Predefined user roles

network-admin
network-operator

Examples

```
# Display TCP packet compression statistics.
<Sysname> display waas statistics tcp compress
Bytes in           : 42413368 bytes
Bytes out          : 29132703 bytes
Saved bandwidth ratio : 31%
Compressed packet ratio: 100%
```

Table 72 Command output

Field	Description
Saved bandwidth ratio	(Number of input bytes–number of output bytes)/Number of input bytes.
Compressed packet ratio	Number of compressed packets/Total number of packets.

Related commands

reset waas statistics tcp compress

reset waas statistics tcp compress

Use **reset waas statistics udp compress** to clear TCP packet compression statistics.

Syntax

reset waas statistics tcp compress

Views

User view

Predefined user roles

network-admin

Examples

```
# Clear TCP packet compression statistics.
<Sysname> reset waas statistics udp compress
```

Related commands

display waas statistics tcp compress

waas tcp

Use **waas tcp** to enable TCP packet compression or decompression.

Use **undo waas tcp** to disable TCP packet compression or decompression.

Syntax

waas tcp { compress [max *max-number*] | decompress }

undo waas tcp

Default

TCP packet compression and decompression is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

compress: Enables TCP packet compression.

max *max-number*: Specifies the maximum number of TCP packets to be compressed per time, in the number of 2 to 20. The default is 5.

decompress: Enables TCP packet decompression.

Usage guidelines

This command takes effect only on TCP packets with the destination IP address and destination port number specified in the **waas tcp destination** command.

Enable TCP packet compression on the upstream device and enable TCP packet decompression on the downstream device. The upstream device compresses packets and forwards them to the downstream device. The downstream device decompresses the received packets and then forwards them.

You can enable TCP packet compression or decompression for the same destination IP address, but not both.

Examples

```
# Enables TCP packet compression and set the maximum number of TCP packets to be compressed to 8.
```

```
<Sysname> system-view
```

```
[Sysname] waas tcp compress max 8
```

Related commands

waas tcp destination

waas tcp destination

Use **waas tcp destination** to specify the destination IP address and destination port number of TCP packets to be compressed or decompressed.

Use **undo waas tcp destination** to remove the specified destination IP address and destination port number.

Syntax

waas tcp destination { *ip-address* **port** *port-number* | **object-group** *ip-object-group-name* **port** **object-group** *port-object-group-name* }

undo waas tcp destination { *ip-address* **port** *port-number* | **object-group** }

Default

No destination IP address and destination port number are specified.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the destination IP address of TCP packets to be compressed or decompressed.

port port-number: Specifies the destination port number of TCP packets, in the range of 1 to 65535.

object-group ip-object-group-name: Specifies an IP address object group by its name to match the destination IP address of TCP packets, a case-insensitive string of 1 to 63 characters.

port object-group port-object-group-name: Specifies a port object group by its name to match the destination port number of TCP packets, a case-insensitive string of 1 to 63 characters.

Usage guidelines

TCP packet compression and decompression takes effect only on TCP packets with the destination IP address and destination port number specified in this command.

You can execute this command multiple times to specify multiple IP address-port number pairs.

In matching TCP packets, object groups have higher priority than the specified IP address and port number.

Examples

Specify that TCP packets with destination IP address 172.16.105.50 and destination port number 8000 are compressed.

```
<Sysname> system-view
[Sysname] waas tcp compress
[Sysname] waas tcp destination 172.16.105.50 port 8000
```

Specify IP address object group **group1** and port object group **group2** to match TCP packets.

```
<Sysname> system-view
[Sysname] waas tcp compress
[Sysname] waas tcp destination ip-address object-group group1 port object-group group2
```

Related commands

waas tcp

New feature: Preferring routes learned from a peer or peer group during optimal route selection

Preferring routes learned from a peer or peer group during optimal route selection

About this task

By default, BGP selects an optimal route based on the predefined route selection rules. It does not prefer routes learned from any peer or peer groups during optimal route selection.

After you perform this task, routes learned from the specified peer or peer group take precedence over other routes if these routes have the same prefix. BGP uses this rule to continue route selection

if it fails to select an optimal route by using the peer type selection rule. If BGP still fails route selection, it uses the IGP metric selection rule to select an optimal route.

Procedure (IPv4 unicast/multicast address family)

1. Enter system view.

system-view

2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, or BGP IPv4 multicast address family view.

- o Execute the following commands in sequence to enter BGP IPv4 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv4 [**unicast**]

- o Execute the following commands in sequence to enter BGP-VPN IPv4 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

ip vpn-instance *vpn-instance-name*

address-family ipv4 [**unicast**]

- o Execute the following commands in sequence to enter BGP IPv4 multicast address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv4 multicast

3. Prefer routes learned from the specified peer or peer group during optimal route selection.

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }

high-priority

By default, BGP does not prefer routes learned from any peer or peer groups during optimal route selection.

The *ipv6-address* [*prefix-length*] argument is supported only in BGP IPv4 unicast address family view.

Procedure (IPv6 unicast/multicast address family)

1. Enter system view.

system-view

2. Enter BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, or BGP IPv6 multicast address family view.

- o Execute the following commands in sequence to enter BGP IPv6 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv6 [**unicast**]

- o Execute the following commands in sequence to enter BGP-VPN IPv6 unicast address family view:

bgp *as-number* [**instance** *instance-name*]

ip vpn-instance *vpn-instance-name*

address-family ipv6 [**unicast**]

- o Execute the following commands in sequence to enter BGP IPv6 multicast address family view:

bgp *as-number* [**instance** *instance-name*]

address-family ipv6 multicast

3. Prefer routes learned from the specified peer or peer group during optimal route selection.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **high-priority**

By default, BGP does not prefer routes learned from any peer or peer groups during optimal route selection.

The *ipv4-address* [*mask-length*] argument is supported only in BGP IPv6 unicast address family view.

Procedure (BGP IPv4 MDT address family)

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP IPv4 MDT address family view.
address-family ipv4 mdt
4. Prefer routes learned from the specified peer or peer group during optimal route selection.
peer { *group-name* | *ipv4-address* [*mask-length*] } **high-priority**
By default, BGP does not prefer routes learned from any peer or peer groups during optimal route selection.

Procedure (BGP IPv4 MVPN address family)

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Create a BGP MVPN peer and specify its AS number.
peer *ipv4-address* **as-number** *as-number*
4. Create BGP IPv4 MVPN address family and enter its view.
address-family ipv4 mvpn
5. Enable BGP to exchange BGP IPv4 MVPN routing information with the dynamic IPv4 peers.
peer *ipv4-address* *mask-length* **enable**
By default, BGP cannot exchange BGP IPv4 MVPN routing information with dynamic IPv4 peers.
6. (Optional.) Disable route target filtering for BGP IPv4 MVPN routes.
undo policy vpn-target
By default, a PE performs route target filtering for received BGP IPv4 MVPN routes.
7. (Optional.) Prefer routes learned from the specified peer or peer group during optimal route selection.
peer { *group-name* | *ipv4-address* [*mask-length*] } **high-priority**
By default, BGP does not prefer routes learned from any peer or peer groups during optimal route selection.

Command reference

peer high-priority

Use **peer high-priority** to set a high priority for BGP routes learned from a peer or peer group during optimal route selection.

Use **undo peer high-priority** to remove the configuration.

Syntax

In BGP IPv6 unicast address family view/BGP VPNv4 address family view/BGP LS address family view/BGP VPNv6 address family view/BGP EVPN address family view/BGP IPv4 flowspec address family view/BGP IPv6 flowspec address family view/BGP-VPN IPv4 flowspec address family view/BGP-VPN IPv6 flowspec address family view/BGP VPNv4 flowspec address family view/BGP VPNv6 flowspec address family view:

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] } high-priority
```

```
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] } high-priority
```

In In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP-VPN VPNv4 address family view/BGP IPv4 multicast address family view/BGP IPv4 MDT address family view/BGP IPv4 RT filter address family view/BGP IPv4 MVPN address family view/BGP IPv4 SR policy address family view:

```
peer { group-name | ipv4-address [ mask-length ] } high-priority
```

```
undo peer { group-name | ipv4-address [ mask-length ] } high-priority
```

In BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view/BGP IPv6 SR policy address family view:

```
peer { group-name | ipv6-address [ prefix-length ] } high-priority
```

```
undo peer { group-name | ipv6-address [ prefix-length ] } high-priority
```

Default

BGP does not prefer routes learned from any peer or peer groups during optimal route selection.

Views

BGP IPv4 unicast address family view

BGP IPv6 unicast address family view

BGP IPv4 multicast address family view

BGP IPv6 multicast address family view

BGP LS address family view

BGP VPNv4 address family view/BGP VPNv6 address family view/BGP-VPN VPNv4 address family view

BGP-VPN IPv4 unicast address family view/BGP-VPN IPv6 unicast address family view

BGP-VPN LS address family view

BGP EVPN address family view

BGP IPv4 RT filter address family view

BGP IPv4 flowspec address family view/BGP IPv6 flowspec address family view

BGP-VPN IPv4 flowspec address family view/BGP-VPN IPv6 flowspec address family view
BGP VPNv4 flowspec address family view/BGP VPNv6 flowspec address family view
BGP IPv4 MVPN address family view
BGP IPv4 MDT address family view
BGP IPv4 SR policy address family view/BGP IPv6 SR policy address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP prefers routes learned from all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet in this command, BGP prefers routes learned from all dynamic peers in the subnet.

Usage guidelines

Routes learned from the specified peer or peer group take precedence over routes learned from other peers or peer groups if these routes have the same prefix. BGP uses this rule to continue route selection if it fails to select an optimal route by using the peer type selection rule. If BGP still fails route selection, it uses the IGP metric selection rule to select an optimal route.

Examples

In BGP IPv4 unicast address family view, prefer BGP routes learned from peer group **test** during optimal route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer test high-priority
```

New feature: Configuring the BGP Additional Paths feature

Configuring the BGP Additional Paths feature

About this task

On a large-scale network, a route reflector can receive multiple BGP routes with the same prefix. By default, BGP advertises only one optimal route. When the optimal route fails, traffic forwarding will be interrupted until route convergence completes.

To resolve this issue, configure the BGP Additional Paths (Add-Path) feature on the route reflector. This feature enables the device to advertise multiple routes with the same prefix to a peer or peer group. On receipt of these routes, the peer generates multiple links to the same destination network.

When the optimal link fails, another link can take over to forward traffic, which enhances the reliability of data transmission.

Restrictions and guidelines

BGP Additional Paths capabilities include the sending capability and the receiving capability. You can enable either of the sending and receiving capabilities or both on a peer. For two BGP peers to successfully negotiate the Additional Paths capabilities, make sure one end has the sending capability and the other end has the receiving capability.

Procedure (IPv4 unicast address family)

1. Enter system view.
system-view
2. Enter BGP IPv4 unicast address family view or BGP-VPN IPv4 unicast address family view.
 - Execute the following commands in sequence to enter BGP IPv4 unicast address family view:
bgp as-number [instance instance-name]
address-family ipv4 [unicast]
 - Execute the following commands in sequence to enter BGP-VPN IPv4 unicast address family view:
bgp as-number [instance instance-name]
ip vpn-instance vpn-instance-name
address-family ipv4 [unicast]
3. Configure the BGP Additional Paths capabilities.
peer { group-name | ipv4-address [make-length] } additional-paths { receive | send }
*
By default, no BGP Additional Paths capabilities are configured.
4. Set the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group.
peer { group-name | ipv4-address [make-length] } advertise additional-paths best number
By default, a maximum number of one Add-Path optimal route can be advertised to a peer or peer group.
5. Set the maximum number of Add-Path optimal routes that can be advertised to all peers.
additional-paths select-best best-number
By default, a maximum number of one Add-Path optimal route can be advertised to all peers.

Procedure (IPv6 unicast address family)

1. Enter system view.
system-view
2. Enter BGP IPv6 unicast address family view or BGP-VPN IPv6 unicast address family view.
 - Execute the following commands in sequence to enter BGP IPv6 unicast address family view:
bgp as-number [instance instance-name]
address-family ipv6 [unicast]
 - Execute the following commands in sequence to enter BGP-VPN IPv6 unicast address family view:
bgp as-number [instance instance-name]
ip vpn-instance vpn-instance-name

address-family ipv6 [unicast]

3. Configure the BGP Additional Paths capabilities.

- In BGP IPv6 unicast address family view:

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
additional-paths { receive | send } *
```

- In BGP-VPN IPv6 unicast address family view:

```
peer { group-name | ipv6-address [ prefix-length ] } additional-paths { receive |  
send } *
```

By default, no BGP Additional Paths capabilities are configured.

4. Set the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group.

- In BGP IPv6 unicast address family view:

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
advertise additional-paths best number
```

- In BGP-VPN IPv6 unicast address family view:

```
peer { group-name | ipv6-address [ prefix-length ] } advertise additional-paths  
best number
```

By default, a maximum number of one Add-Path optimal route can be advertised to a peer or peer group.

5. Set the maximum number of Add-Path optimal routes that can be advertised to all peers.

```
additional-paths select-best best-number
```

By default, a maximum number of one Add-Path optimal route can be advertised to all peers.

Command reference

additional-paths select-best

Use **additional-paths select-best** to set the maximum number of Add-Path optimal routes that can be advertised to all peers.

Use **undo additional-paths select-best** to restore the default.

Syntax

```
additional-paths select-best best-number
```

```
undo additional-paths select-best
```

Default

A maximum number of one Add-Path optimal route can be advertised to all peers.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP-VPN VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

best-number: Specifies the maximum number of Add-Path optimal routes that can be advertised to all peers. The value range for the *best-number* argument is 2 to 64.

Usage guidelines

The number of optimal routes cannot exceed the maximum number of Add-Path optimal routes that can be advertised to all peers.

Examples

In BGP IPv4 unicast address family view, set the maximum number to 3 for Add-Path optimal routes that can be advertised to all peers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] additional-paths select-best 3
```

Related commands

peer additional-paths

peer advertise additional-paths best

peer additional-paths

Use **peer additional-paths** to configure the BGP Additional Paths capabilities.

Use **undo peer additional-paths** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP-VPN VPNv4 address family view:

```
peer { group-name | ipv4-address [ mask-length ] } additional-paths { receive | send } *
undo peer { group-name | ipv4-address [ mask-length ] } additional-paths { receive | send } *
```

In BGP-VPN IPv6 unicast address family view:

```
peer { group-name | ipv6-address [ prefix-length ] } additional-paths { receive | send } *
undo peer { group-name | ipv6-address [ prefix-length ] } additional-paths { receive | send } *
```

In BGP VPNv4 address family view/BGP IPv6 unicast address family view/BGP VPNv6 address family view/BGP EVPN address family view:

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] } additional-paths { receive | send } *
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] } additional-paths { receive | send } *
```

Default

No BGP Additional Paths capabilities are configured.

Views

BGP IPv4 unicast address family view
BGP-VPN IPv4 unicast address family view
BGP VPNv4 address family view
BGP-VPN VPNv4 address family view
BGP IPv6 unicast address family view
BGP-VPN IPv6 unicast address family view
BGP VPNv6 address family view
BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command configures the BGP Additional Paths capabilities for all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command configures the BGP Additional Paths capabilities for all dynamic peers in the subnet.

receive: Enables the BGP additional path receiving capability.

send: Enables the BGP additional path sending capability.

Usage guidelines

For two BGP peers to successfully negotiate the Additional Paths capabilities, make sure one end has the sending capability and the other end has the receiving capability.

Examples

In BGP IPv4 unicast address family view, enable the BGP additional path receiving capability.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 additional-paths receive
```

peer advertise additional-paths best

Use **peer advertise additional-paths best** to set the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group.

Use **undo peer advertise additional-paths best** to remove the configuration.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP-VPN VPNv4 address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise additional-paths best number**

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise additional-paths best**

In BGP-VPN IPv6 unicast address family view:

peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise additional-paths best number**

undo peer { *group-name* | *ipv6-address* [*prefix-length*] } **advertise additional-paths best**

In BGP VPNv4 address family view/BGP IPv6 unicast address family view/BGP VPNv6 address family view/BGP EVPN address family view:

peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise additional-paths best number**

undo peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **advertise additional-paths best**

Default

A maximum number of one Add-Path optimal route can be advertised to a peer or peer group.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP-VPN VPNv4 address family view

BGP IPv6 unicast address family view

BGP-VPN IPv6 unicast address family view

BGP VPNv6 address family view

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must have been created.

ipv4-address: Specifies a peer by its IPv4 address. The peer must have been created.

mask-length: Specifies a mask length in the range of 0 to 32. You can use the *ipv4-address* and *mask-length* arguments together to specify a subnet. If you specify a subnet, this command sets the maximum number of Add-Path optimal routes that can be advertised to all dynamic peers in the subnet.

ipv6-address: Specifies a peer by its IPv6 address. The peer must have been created.

prefix-length: Specifies a prefix length in the range of 0 to 128. You can use the *ipv6-address* and *prefix-length* arguments together to specify a subnet. If you specify a subnet, this command sets the maximum number of Add-Path optimal routes that can be advertised to all dynamic peers in the subnet.

number: Specifies the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group, in the range of 2 to 64.

Usage guidelines

If the number of Add-Path optimal routes advertised to a peer or peer group exceeds the number of optimal routes, the number of optimal routes takes effect.

Examples

In BGP IPv4 unicast address family view, set the maximum number to 3 for Add-Path optimal routes that can be advertised to peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 advertise additional-paths best 3
```

Related commands

additional-paths select-best

peer additional-paths

New feature: Allowing the RR to change the attributes of routes to be reflected

Allowing the RR to change the attributes of routes to be reflected

1. Enter system view.
system-view
2. Enter BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, BGP IPv4 multicast address family view, BGP IPv6 unicast address family view, and BGP IPv6 multicast address family view.
 - o Enter BGP IPv4 unicast address family view.
bgp as-number [instance instance-name]
address-family ipv4 [unicast]
 - o Enter BGP-VPN IPv4 unicast address family view.
bgp as-number [instance instance-name]
ip vpn-instance vpn-instance-name
address-family ipv4 [unicast]
 - o Enter BGP IPv4 multicast address family view.
bgp as-number [instance instance-name]
address-family ipv4 multicast
 - o Enter BGP IPv6 unicast address family view.
bgp as-number [instance instance-name]
address-family ipv6 [unicast]
 - o Enter BGP IPv6 multicast address family view.
bgp as-number [instance instance-name]
address-family ipv6 multicast
3. (Optional.) Allow the RR to change the attributes of routes to be reflected.

reflect change-path-attribute

By default, the RR cannot change the attributes of routes to be reflected.

This command is not supported in BGP IPv4 multicast address family view.

Command reference

reflect change-path-attribute

Use **reflect change-path-attribute** to enable the route reflector to change the attributes of routes to be reflected.

Use **undo reflect change-path-attribute** to restore the default.

Syntax

reflect change-path-attribute

undo reflect change-path-attribute

Default

A route reflector cannot change the attributes of routes to be reflected.

Views

BGP IPv4 unicast address family view

BGP-VPN IPv4 unicast address family view

BGP VPNv4 address family view

BGP IPv6 unicast address family view

BGP VPNv6 address family view

Predefined user roles

network-admin

Usage guidelines

By default, the route reflector does not change the attributes of routes before route reflection to avoid routing loops. When you replan network traffic, you can use this command to allow the route reflector to change the attributes of the routes to be reflected.

After you configure this command, all route attribute modification settings can take effect on the routes to be reflected.

Examples

In BGP IPv4 unicast address family view, enable the route reflector to change the attributes of routes to be reflected.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] address-family ipv4 unicast
```

```
[Sysname-bgp-default-ipv4] reflect change-path-attribute
```

Related commands

peer reflect-client

reflect between-clients

New feature: Configuring packet duplication optimization

Configuring packet duplication optimization

1. Enter system view.
system-view
2. Create a WAAS policy and enter WAAS policy view.
waas policy *policy-name*
By default, a predefined WAAS policy named **waas_default** exists.
3. Specify a WAAS class and enter WAAS policy class view.
class *class-name* [**insert-before** *existing_class*]
By default, no WAAS class is specified.
4. Configure the packet duplication optimization action.
optimize packet-dup

Command reference

New command: display waas statistics packet-dup

Use **display waas statistics packet-dup** to display packet statistics of packet duplication.

Syntax

display waas statistics packet-dup { **ipv4** | **ipv6** }

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

ipv4: Specifies IPv4 packets.

ipv6: Specifies IPv6 packets.

Examples

Display packet statistics of IPv4 packet duplication.

```
<Sysname> display waas statistics packet-dup ipv4
```

Packet Duplication:

Original packets	: 522

Duplicated packets	: 522

Non-duplicated packets due to fragmentation	: 0

Packets exceeding MTU	: 0

Packet Redundancy:

```

Passed packets                                     :200
Discarded packets                                 :199
Packet Order Preservation:
  In-order packets sent                           :200
  Out-of-order packets sent                       :19
  Out-of-order packets cached                     :40
  Cached packets sent in order                    :40
  Cache failed packets sent                       :0
  Cached packets sent on timeout                  :0
  Out-of-order fragmented packets sent            :10
  Out-of-order fragmented packets cached          :0
  Cached fragmented packets sent in order         :0
  Cached fragmented packets sent on timeout       :0

```

Table 73 Command output

Field	Description
Packet Duplication	Packet statistics for packet duplication on the sender.
Original packets	Number of original packets.
Duplicated packets	Number of duplicated packets.
Non-duplicated packets due to fragmentation	Number of non-duplicated packets due to fragmentation.
Packets exceeding MTU	Number of packets with the length exceeding the MTU.
Packet Redundancy	Packet statistics for packet redundancy on the receiver.
Passed packets	Number of passed packets.
Discarded packets	Number of duplicated packets dropped.
Packet Order Preservation	Packet statistics for packet order preservation on the receiver.
In-order packets sent	Number of in-order packets sent.
Out-of-order packets sent	Number of out-of-order packets sent.
Out-of-order packets cached	Number of out-of-order packets cached.
Cached packets sent in order	Number of cached packets sent in order.
Cache failed packets sent	Number of packets sent after failed to be cached.
Cached packets sent on timeout	Number of cached packets sent out of order after timeout.
Out-of-order fragmented packets sent	Number of out-of-order fragmented packets sent.
Out-of-order fragmented packets cached	Number of out-of-order fragmented packets cached.
Cached fragmented packets sent in order	Number of cached fragmented packets sent in order.

Related commands

reset waas statistics packet-dup

Modified command: optimize

Old syntax

In WAAS policy class view:

optimize { fec | tfo [dre | lz] * }

undo optimize

In WAAS policy RTP class view:

optimize fec

undo optimize

New syntax

In WAAS policy class view:

optimize { fec | packet-dup | tfo [dre | lz] * }

undo optimize

In WAAS policy RTP class view:

optimize fec

undo optimize

Change description

Before modification: The **packet-dup** keyword is not supported.

After modification: The **packet-dup** keyword is supported.

packet-dup: Specifies the packet duplication optimization action.

New command: reset waas statistics packet-dup

Use **reset waas statistics packet-dup** to clear packet statistics of packet duplication.

Syntax

reset waas statistics packet-dup { ipv4 | ipv6 }

Views

User view

Predefined user roles

network-admin

Parameters

ipv4: Specifies IPv4 packets.

ipv6: Specifies IPv6 packets.

Examples

Clear packet statistics of IPv4 packet duplication.

<Sysname> reset waas statistics packet-dup ipv4

Related commands

display waas statistics packet-dup

New feature: Specify an ACL to match the TCP or UDP packets that can be compressed or decompressed

Specify an ACL to match the TCP or UDP packets that can be compressed or decompressed

1. Enter system view.
system-view
2. Specify an ACL to match the TCP packets that can be compressed or decompressed.
waas tcp acl { *acl-number* | **name** *acl-name* }
By default, no ACL is specified.
3. Specify an ACL to matched UDP messages that can be compressed or decompressed.
waas udp acl { *acl-number* | **name** *acl-name* }
By default, no ACL is specified.

Command reference

waas tcp acl

Use **waas tcp acl** to specify an ACL to match the TCP packets that can be compressed or decompressed.

Use **undo waas tcp acl** to restore the default.

Syntax

waas tcp acl { *acl-number* | **name** *acl-name* }

undo waas tcp acl

Default

No ACL is specified.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for basic ACLs or in the range of 3000 to 3999 for advanced ACLs.

name *acl-name*: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter. To avoid confusion, make sure the argument is not **all**.

Usage guidelines

Only TCP packets matching the specified ACL are compressed or decompressed.

After you specify an ACL to match TCP packets, the destination IP address and destination port number specified in the **waas tcp destination** command do not take effect.

When you specify an ACL when executing this command, follow these restrictions and guidelines:

- If the ACL does not exist or the ACL does not contain any rules, no TCP packets will be compressed or decompressed.
- If a rule in the ACL is configured with the **vpn-instance** keyword, the rule takes effect only on VPN packets. If the rule is not configured with the **vpn-instance** keyword, the rule takes effect only on public network packets.

Examples

Specify ACL 2001 to match the TCP packets that can be compressed or decompressed.

```
<Sysname> system-view
[Sysname] waas tcp acl 2001
```

Related commands

waas tcp

waas tcp destination

waas udp acl

Use **waas udp acl** to specify an ACL to match the UDP messages that can be compressed or decompressed.

Use **undo waas udp acl** to restore the default.

Syntax

waas udp acl { *acl-number* | **name** *acl-name* }

undo waas udp acl

Default

No ACL is specified.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999 for basic ACLs or in the range of 3000 to 3999 for advanced ACLs.

name acl-name: Specifies an ACL by its name, a case-insensitive string of 1 to 63 characters. The ACL name must start with an English letter. To avoid confusion, make sure the argument is not **all**.

Usage guidelines

Only UDP messages matching the specified ACL are compressed or decompressed.

After you specify an ACL to match UDP messages, the destination IP address and destination port number specified in the **waas udp destination** command do not take effect.

When you specify an ACL when executing this command, follow these restrictions and guidelines:

- If the ACL does not exist or the ACL does not contain any rules, no UDP messages will be compressed or decompressed..

- If a rule in the ACL is configured with the **vpn-instance** keyword, the rule takes effect only on VPN packets. If the rule is not configured with the **vpn-instance** keyword, the rule takes effect only on public network packets.

Examples

Specify ACL 2001 to match the UDP messages that can be compressed or decompressed.

```
<Sysname> system-view
```

```
[Sysname] waas udp acl 2001
```

Related commands

waas udp

waas udp destination

New feature: Configuring packet duplication parameters

Configuring packet duplication optimization parameters

About this task

When packet duplication optimization is enabled on the device, the sender replicates the packets to be sent and selects an additional path reachable to the destination as the forwarding path for the packets. After receiving the packets, the receiver reorders the packets to ensure the integrity and continuity of the packets.

The sender can select a path by using the packet duplication algorithm, by using the RIR feature, or by using a static path, with different priorities.

- If packet duplication RIR is enabled, the device selects a path based on the link priority, link quality, and link bandwidth. This method has the highest priority.
- If a path is manually specified on the device and no path calculated by using the packet duplication RIR algorithm exists, the device uses the manually specified path. A manually specified path has higher priority than the path selected by using the packet duplication algorithm.
- If the device detects that neither a path selected by using the packet duplication RIR feature nor a manually specified path exists, it selects the first path in the routing table that has the same cost as the original path by using the packet duplication algorithm.

With the packet reorder feature, the sender numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n, and then replicates and forwards the packets. The receiver discards the packets with the same sequence number and reorders them before forwarding them. If no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Restrictions and guidelines

Packet duplication RIR takes effect only if RIR is enabled on the device. For more information about RIR, see RIR configuration in *Layer 3—IP Routing Configuration Guide*.

Make sure an SDWAN tunnel exists for a manually specified packet duplication path. If the same SDWAN tunnel is configured as the packet duplication path multiple times, the most recent configuration takes effect. If multiple paths are specified for the same destination, only one path will be selected as the packet duplication path by using a specific algorithm. Manually specifying a packet duplication path is available only in an SDWAN network.

Enabling packet duplication RIR

1. Enter system view.
system-view
2. Create a WAAS policy and enter WAAS policy view.
waas policy *policy-name*
3. Specify a class and enter WAAS policy class view.
class *class-name* [**insert-before** *existing_class*]
4. Enable packet duplication RIR.
packet-dup rir enable
By default, packet duplication RIR is disabled.

Manually specifying a packet duplication path in an SDWAN network

1. Enter system view.
system-view
2. Manually specify a packet duplication path in an SDWAN network.
waas packet-dup sdwan static-path { **destination-ip** *dest-ipv4-address* { *dest-mask-length* | *dest-mask* } | **destination-ipv6** *dest-ipv6-address* *dest-prefix-length* } [**vpn-instance** *vpn-instance-name*] **interface** *interface-type* *interface-number* **peer-site-id** *peer-site-id* **peer-device-id** *peer-device-id* **peer-interface-id** *peer-interface-id* [**priority** *priority*]
By default, no packet duplication path is manually specified in an SDWAN network.

Setting the packet duplication reorder timeout timer

1. Enter system view.
system-view
2. Create a WAAS policy and enter WAAS policy view.
waas policy *policy-name*
3. Specify a class and enter WAAS policy class view.
class *class-name* [**insert-before** *existing_class*]
4. Set the packet duplication reorder timeout timer.
packet-dup reorder timeout *timeout*
By default, the packet duplication reorder timeout timer is 100 ms.

Command reference

packet-dup reorder timeout

Use **packet-dup reorder timeout** to set the packet duplication reorder timeout timer.

Use **undo packet-dup reorder timeout** to restore the default.

Syntax

packet-dup reorder timeout *timeout*

undo packet-dup reorder timeout

Default

The packet duplication reorder timeout timer is 100 ms.

Views

WAAS policy class view

Predefined user roles

network-admin

Parameters

timeout: Specifies the packet duplication reorder timeout timer, in the range of 1 to 65535 milliseconds.

Usage guidelines

With the packet reorder feature, the sender numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n, and then replicates and forwards the packets. The receiver discards the packets with the same sequence number and reorders them before forwarding them. If no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Examples

Set the packet duplication reorder timeout timer to 100 milliseconds for WAAS class 1.

```
<Sysname> system-view
```

```
[Sysname] waas policy 1
```

```
[Sysname-waaspolicy-1] class 1
```

```
[Sysname-waaspolicy-1-1] packet-dup reorder timeout 100
```

packet-dup rir enable

Use **packet-dup rir enable** to enable packet duplication RIR.

Use **undo packet-dup rir enable** to disable packet duplication RIR.

Syntax

packet-dup rir enable

undo packet-dup rir enable

Default

Packet duplication RIR is disabled.

Views

WAAS policy class view

Predefined user roles

network-admin

Usage guidelines

With packet duplication RIR enabled, the device selects a path based on the link priority, link quality, and link bandwidth.

Packet duplication RIR takes effect only if RIR is enabled on the device. For more information about RIR, see RIR configuration in *Layer 3—IP Routing Configuration Guide*.

The sender can select a path by using the packet duplication RIR feature or by using a static path.

- If a path is manually specified on the device and a path calculated by using the packet duplication RIR algorithm exists, the device uses the path selected by using the packet duplication RIR algorithm.
- If the device detects that neither a path selected by using the packet duplication RIR feature nor a manually specified path exists, it selects the first path in the routing table that has the same cost as the original path by using the packet duplication algorithm.

Examples

```
# Enable packet duplication RIR for WAAS policy class 1.
<Sysname> system-view
[Sysname] waas policy 1
[Sysname-waaspolicy-1] class 1
[Sysname-waaspolicy-1-1] packet-dup rir enable
```

Related commands

optimize

rir (*Layer 3—IP Routing Command Reference*)

rir sdwan (*Layer 3—IP Routing Command Reference*)

reset waas statistics load-balance

Use **reset waas statistics load-balance** to clear load balancing packet statistics.

Syntax

reset waas statistics load-balance { ipv4 | ipv6 }

Views

User view

Predefined user roles

network-admin

Parameters

ipv4: Clears IPv4 packet statistics.

ipv6: Clears IPv6 packet statistics.

Usage guidelines

This command is supported only for packets load shared in per-packet mode.

Examples

```
# Clears IPv4 load balancing packet statistics.
```

```
<Sysname> reset waas statistics load-balance ipv4
```

Related commands

display waas statistics load-balance

waas packet-dup sdwan static-path

Use **waas packet-dup sdwan static-path** to manually specify a packet duplication path in an SDWAN network.

Use **undo waas packet-dup sdwan static-path** to remove a packet duplication path in an SDWAN network.

Syntax

waas packet-dup sdwan static-path { **destination-ip** *dest-ipv4-address* { *dest-mask-length* | *dest-mask* } | **destination-ipv6** *dest-ipv6-address* *dest-prefix-length* } [**vpn-instance** *vpn-instance-name*] **interface** *interface-type* *interface-number* **peer-site-id** *peer-site-id* **peer-device-id** *peer-device-id* **peer-interface-id** *peer-interface-id* [**priority** *priority*]

undo waas packet-dup sdwan static-path [{ **destination-ip** *dest-ipv4-address* { *dest-mask-length* | *dest-mask* } | **destination-ipv6** *dest-ipv6-address* *dest-prefix-length* } [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type* *interface-number*] [**peer-site-id** *peer-site-id* **peer-device-id** *peer-device-id* **peer-interface-id** *peer-interface-id*] [**priority** *priority*]]

Default

No packet duplication path exists in an SDWAN network.

Views

System view

Predefined user roles

network-admin

Parameters

destination-ip *dest-ip-address*: Specifies a destination IPv4 address in dotted decimal notation.

dest-mask-length: Specifies a mask length for the destination IPv4 address, in the range of 0 to 32.

dest-mask: Specifies a subnet mask for the destination IPv4 address, in dotted decimal notation.

destination-ipv6 *dest-ipv6-address*: Specifies a destination IPv6 address.

dest-prefix-length: Specifies a prefix length for the destination IPv6 address, in the range of 1 to 128.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters.

interface *interface-type* *interface-number*: Specifies an interface by its type and number. Only tunnel interfaces are supported.

peer-site-id *peer-site-id*: Specifies a site ID in the range of 1 to 65535.

peer-device-id *peer-device-id*: Specifies a device ID in the range of 1 to 255.

peer-interface-id *peer-interface-id*: Specifies an interface ID in the range of 1 to 255.

priority *priority*: Specifies a priority for the static path, in the range of 1 to 255. The default priority is 60. A larger value indicates a higher priority.

Usage guidelines

Make sure the specified SDWAN tunnel already exists. To view the SDWAN tunnels on the device, execute the **display sdwan tte connection** command.

If the same SDWAN tunnel is configured as the packet duplication path multiple times, the most recent configuration takes effect. If multiple paths are specified for the same destination, only one path will be selected as the packet duplication path by using a specific algorithm.

The sender can select a path by using the packet duplication RIR feature or by using a static path.

- If a path is manually specified on the device and a path calculated by using the packet duplication RIR algorithm exists, the device uses the path selected by using the packet duplication RIR algorithm.
- If the device detects that neither a path selected by using the packet duplication RIR feature nor a manually specified path exists, it selects the first path in the routing table that has the same cost as the original path by using the packet duplication algorithm.

If you do not specify any keywords when executing the **undo waas packet-dup sdwan static-path** command, the command deletes all manually specified packet duplication paths.

This command is available only in an SDWAN network.

Examples

Manually specify a packet duplication path in an SDWAN network.

```
<Sysname> system-view
```

```
[Sysname] waas packet-dup sdwan static-path ip 200.1.1.0 24 vpn-instance vpn-1 local tunnel  
1 peer site-id 2 device-id 3 interface-id 5 priority 50
```

Related commands

display sdwan tte connection (*SDWAN Command Reference*)

New feature: Setting the reorder timeout timer for load balancing packets

Setting the reorder timeout timer for load balancing packets

About this task

With load balancing enabled on the device, the sender forwards the packets on all paths with the same cost to the destination. This can cause packet disorder on the receiver. WAAS numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n. The receiver reorders and forwards the packets. With the load balancing packet reorder timeout timer set, if no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Procedure

1. Enter system view.
system-view
2. Set the reorder timeout timer for load balancing packets.
waas load-balance reorder timeout *timeout*

By default, the reorder timeout timer is 100 ms for load balancing packets.

Command reference

display waas statistics load-balance

Use **display waas statistics load-balance** to display load sharing packet statistics.

Syntax

display waas statistics load-balance { ipv4 | ipv6 }

Views

Any view

Predefined user roles

- network-admin
- network-operator

Parameters

- ipv4**: Displays IPv4 packet statistics.
- ipv6**: Displays IPv6 packet statistics.

Usage guidelines

This command is supported only for packets load shared in per-packet mode.

Examples

```
# Display IPv4 load sharing packet statistics.
<Sysname> display waas statistics load-balance ipv4
Packet Order Preservation:
  In-order packets sent                               :200
  Out-of-order packets sent                           :19
  Out-of-order packets cached                         :40
  Cached packets sent in order                        :40
  Cache failed packets sent                           :0
  Cached packets sent on timeout                      :0
  Out-of-order fragmented packets sent                :1
  Out-of-order fragmented packets cached              :3
  Cached fragmented packets sent in order              :3
  Cached fragmented packets sent on timeout            :3
```

Table 74 Command output

Field	Description
Packet Order Preservation	Packet statistics for packet order preservation on the receiver.
In-order packets sent	Number of in-order packets sent.
Out-of-order packets sent	Number of out-of-order packets sent.
Out-of-order packets cached	Number of out-of-order packets cached.
Cached packets sent in order	Number of cached packets sent in order.
Cache failed packets sent	Number of packets sent after failed to be cached.
Cached packets sent on timeout	Number of cached packets sent out of order after

	timeout.
Out-of-order fragmented packets sent	Number of out-of-order fragmented packets sent.
Out-of-order fragmented packets cached	Number of out-of-order fragmented packets cached.
Cached fragmented packets sent in order	Number of cached fragmented packets sent in order.
Cached fragmented packets sent on timeout	Number of cached fragmented packets sent out of order after timeout.

Related commands

reset waas statistics load-balance

waas load-balance reorder timeout

Use **waas load-balance reorder timeout** to set the reorder timeout timer for load balancing packets.

Use **undo waas load-balance reorder timeout** to restore the default.

Syntax

waas load-balance reorder timeout *timeout*

undo waas load-balance reorder timeout

Default

The reorder timeout timer is 100 ms for load balancing packets.

Views

System view

Predefined user roles

network-admin

Parameters

timeout: Specifies the reorder timeout timer for load balancing packets, in the range of 1 to 65535 milliseconds.

Usage guidelines

With load balancing enabled on the device, the sender forwards the packets on all paths with the same cost to the destination. This can cause packet disorder on the receiver. WAAS numbers the packets to be sent based on the order in which the packets will be sent, for example, 1, 2... n. The receiver reorders and forwards the packets. With the load balancing packet reorder timeout timer set, if no packet with a smaller sequence number is received, the receiver will cache the received packets and send the packets in sequence after a packet with a smaller sequence number arrives. If the receiver does not receive a packet with a smaller sequence number before the reorder timeout timer expires, the receiver will directly send the cached packets.

Examples

Set the reorder timeout timer for load balancing packets.

```
<Sysname> system-view
```

```
[Sysname] waas load-balance reorder timeout 100
```


New feature: Support for the link tag feature

Configuring the IPv6 IS-IS link tag feature

About this task

Set an IPv6 IS-IS link tag for a device (for example, Device A) and enable IPv6 IS-IS link tag inheritance on another device (for example, Device B) to filter routes as follows:

1. Device A advertises the IPv6 IS-IS link tag in LSPs.
2. After receiving the LSPs advertised by Device A, Device B inherits the IPv6 IS-IS link tag advertised by Device A.

If Device B receives multiple link tags from Device A, Device B selects and inherits only one tag.

3. Device B configures the link tag as the route tag for all routes that pass the link.
Then, the route tag can be used for route filtering.

This feature is usually used in Source Address Validation Architecture (SAVA) scenarios to ensure the consistency of IPv6 SAVA entries on multiple gateway devices:

4. Set an IPv6 IS-IS link tag for the customer-side interface on the gateway device that advertises IPv6 SAVA entries.
5. Enable IPv6 IS-IS link tag inheritance on the gateway device that receives IPv6 SAVA entries. The device generates an IPv6 SAVA entry based on a route prefix if the following two tags are the same:
 - The route tag configured by executing the **ipv6 sava import remote-route-tag** command.
 - The IPv6 IS-IS link tag that the route inherits.

For more information about SAVA and IPv6 SAVA entries, see SAVA configuration in *Security Configuration Guide*.

Setting an IPv6 IS-IS link tag for an interface

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Set an IPv6 IS-IS link tag for the interface.
isis ipv6 link-tag *tag*
By default, no IPv6 IS-IS link tag is configured for the interface.

Enabling IPv6 IS-IS link tag inheritance

1. Enter system view.
system-view
2. Enter IS-IS view.
isis [*process-id*] [**vpn-instance** *vpn-instance-name*]
3. Enter IPv6 address family view.
address-family ipv6 [**unicast**]
4. Enable IPv6 IS-IS link tag inheritance.

link-tag inherit enable

By default, IPv6 IS-IS link tag inheritance is disabled.

Command reference

isis ipv6 link-tag

Use **isis ipv6 link-tag** to set an IPv6 IS-IS link tag for an interface.

Use **undo isis ipv6 link-tag** to restore the default.

Syntax

isis ipv6 link-tag *tag*

undo isis ipv6 link-tag

Default

No IPv6 IS-IS link tag is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

tag: Specifies an IPv6 IS-IS link tag in the range of 1 to 4294967295.

Usage guidelines

Execute this command together with the **link-tag inherit enable** command to filter routes based on IPv6 IS-IS link tags.

If you execute this command multiple times on an interface, the most recent configuration takes effect.

Examples

```
# Set the IPv6 IS-IS link tag for interface GigabitEthernet 1/0/1 to 222333.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] isis ipv6 link-tag 222333
```

Related commands

link-tag inherit enable

link-tag inherit enable

Use **link-tag inherit enable** to enable IPv6 IS-IS link tag inheritance.

Use **undo link-tag inherit enable** to disable IPv6 IS-IS link tag inheritance.

Syntax

link-tag inherit enable

undo link-tag inherit enable

Default

IPv6 IS-IS link tag inheritance is disabled.

Views

IS-IS IPv6 unicast address family view

Predefined user roles

network-admin

Usage guidelines

After you execute this command on a device, the device inherits the IPv6 IS-IS link tag in received LSPs. If the device receives multiple link tags from a device, it selects and inherits only one tag. Then, the device configures the link tag as the route tag for all routes that pass the link.

The IPv6 IS-IS link tag feature is usually used in Source Address Validation Architecture (SAVA) scenarios to ensure the consistency of IPv6 SAVA entries on multiple gateway devices:

1. Set an IPv6 IS-IS link tag for the customer-side interface on the gateway device that advertises IPv6 SAVA entries.
2. Enable IPv6 IS-IS link tag inheritance on the gateway device that receives IPv6 SAVA entries. The device generates an IPv6 SAVA entry based on a route prefix if the following two tags are the same:
 - The route tag configured by executing the **ipv6 sava import remote-route-tag** command.
 - The IPv6 IS-IS link tag that the route inherits.

For more information about SAVA, see SAVA configuration in *Security Configuration Guide*.

Examples

In IS-IS process 1, enable IPv6 IS-IS link tag inheritance.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] address-family ipv6
[Sysname-isis-1-ipv6] link-tag inherit enable
```

Related commands

isis ipv6 link-tag

Configuring the OSPFv3 link tag feature

About this task

The interface link tag feature can work together with the link tag inheritance feature to filter routes. For example, you can set an OSPFv3 link tag for Device A and enable OSPFv3 link tag inheritance on Device B to filter routes as follows:

1. Device A advertises the OSPFv3 link tag in E-router LSAs.
2. After receiving the LSAs advertised by Device A, Device B inherits the OSPFv3 link tag advertised by Device A.

If Device B receives multiple link tags from Device A, Device B selects and inherits only one tag.
3. Device B configures the link tag as the route tag for all routes that pass the link.

Then, the route tag can be used for route filtering.

This feature is usually used in Source Address Validation Architecture (SAVA) scenarios to ensure the consistency of IPv6 SAVA entries on multiple gateway devices as follows:

4. Set an OSPFv3 link tag for the customer-side interface on the gateway device that advertises IPv6 SAVA entries.
5. Enable OSPFv3 link tag inheritance on the gateway device that receives IPv6 SAVA entries. The device generates an IPv6 SAVA entry based on a route prefix if the following two tags are the same:
 - The route tag configured by executing the **ipv6 sava import remote-route-tag** command.
 - The OSPFv3 link tag that the route inherits.

For more information about SAVA and IPv6 SAVA entries, see SAVA configuration in *Security Configuration Guide*.

Setting an OSPFv3 link tag for an interface

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Set an OSPFv3 link tag for the interface.
ospfv3 link-tag tag [instance instance-id]
By default, no OSPFv3 link tag is configured for the interface.

Enabling OSPFv3 link tag inheritance

1. Enter system view.
system-view
2. Enter OSPFv3 view.
ospfv3 [*process-id* | **vpn-instance** *vpn-instance-name*] *
3. Enable OSPFv3 link tag inheritance.
link-tag inherit enable
By default, OSPFv3 link tag inheritance is disabled.

Command reference

link-tag inherit enable

Use **link-tag inherit enable** to enable OSPFv3 link tag inheritance.

Use **undo link-tag inherit enable** to disable OSPFv3 link tag inheritance.

Syntax

link-tag inherit enable

undo link-tag inherit enable

Default

OSPFv3 link tag inheritance is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Usage guidelines

After you execute this command on a device, the device inherits the OSPFv3 link tag in received LSPs. If the device receives multiple link tags from a device, it selects and inherits only one tag. Then, the device configures the link tag as the route tag for all routes that pass the link.

This feature is usually used in Source Address Validation Architecture (SAVA) scenarios to ensure the consistency of IPv6 SAVA entries on multiple gateway devices as follows:

1. Set an OSPFv3 link tag for the customer-side interface on the gateway device that advertises IPv6 SAVA entries.
2. Enable OSPFv3 link tag inheritance on the gateway device that receives IPv6 SAVA entries. The device generates an IPv6 SAVA entry based on a route prefix if the following two tags are the same:
 - o The route tag configured by executing the **ipv6 sava import remote-route-tag** command.
 - o The OSPFv3 link tag that the route inherits.

For more information about SAVA and IPv6 SAVA entries, see SAVA configuration in *Security Configuration Guide*.

Examples

In OSPFv3 process 1, enable OSPFv3 link tag inheritance.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] link-tag inherit enable
```

Related commands

ipv6 sava import remote-route-tag (*Security Command Reference*)

ospfv3 link-tag

ospfv3 link-tag

Use **ospfv3 link-tag** to set an OSPFv3 link tag for an interface.

Use **undo ospfv3 link-tag** to restore the default.

Syntax

ospfv3 link-tag tag [**instance** *instance-id*]

undo ospfv3 link-tag [**instance** *instance-id*]

Default

No OSPFv3 link tag is configured for an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

tag: Specifies an OSPFv3 link tag in the range of 1 to 4294967295.

instance *instance-id*: Specifies an instance by its ID in the range of 0 to 255. The default is 0.

Usage guidelines

Execute this command together with the **link-tag inherit enable** command to filter routes based on OSPFv3 link tags.

If you execute this command multiple times on an interface, the most recent configuration takes effect.

Examples

```
# Set the OSPFv3 link tag for interface GigabitEthernet 1/0/1 to 222333.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 link-tag 222333
```

Related commands

link-tag inherit enable

Modified feature: Binding a POS terminal template to an interface and configuring a POS application mapping entry

Feature change description

As from this release, the device supports specifying a POS application template group when you bind a POS terminal template to an interface or configure a POS application mapping entry.

Command changes

Modified command: **posa bind terminal**

Use **posa bind terminal** to bind a POS terminal template to an interface.

Use **undo posa bind terminal** to restore the default.

Old syntax

posa bind terminal *terminal-id* [**app** *app-id*]

undo posa bind terminal

New syntax

posa bind terminal *terminal-id* [**app** *app-id* | **app-group** *app-group-name*]

undo posa bind terminal

Default

No POS terminal template is bound to an interface.

Views

Asynchronous interface view

Physical AM interface view

Physical FCM interface view

Synchronous/asynchronous interface view

Change description

The **app-group** *app-group-name* option is added to the command to specify a POS application template group to be associated with the POS terminal template in transparent mode by its name. The *app-group-name* argument is a case-insensitive string of 1 to 31 characters. The specified application template group must already exist. If no application template group is specified, it indicates that the terminal template operates in nontransparent mode.

Modified command: `posa map`

Use **posa map** to configure POS application mapping entries.

Use **undo posa map** to remove POS application mapping entries.

Old syntax

```
posa map { default | destination des-code | source src-code } * app app-id
```

```
undo posa map { default | destination des-code | source src-code } *
```

New syntax

```
posa map { default | destination des-code | source src-code } * { app app-id | app-group app-group-name }
```

```
undo posa map { default | destination des-code | source src-code } *
```

Default

No POS application mapping entries are configured.

Views

System view

Change description

The **app-group** *app-group-name* option is added to the command to specify a POS application template group by its name. The *app-group-name* argument is a case-insensitive string of 1 to 31 characters. The specified application template group must already exist. If the application template group does not exist, the configuration is allowed but it does not take effect.

Modified feature: Configuring RIR in RIR-SDWAN view, RIR-SDWAN flow template view, and RIR-SDWAN SLA view

Feature change description

As from this release, you can configure RIR in RIR-SDWAN view, RIR-SDWAN flow template view, and RIR-SDWAN SLA view.

Command changes

Modified command: flow priority-based-schedule bandwidth-threshold

Use **flow priority-based-schedule bandwidth-threshold** to set the bandwidth usage thresholds for flow priority-based traffic scheduling.

Use **undo flow priority-based-schedule bandwidth-threshold** to restore the default.

Syntax

flow priority-based-schedule bandwidth-threshold upper *upper-threshold* lower *lower-threshold*

undo flow priority-based-schedule bandwidth-threshold

Default

The bandwidth usage upper threshold is 90% and the bandwidth usage lower threshold is 20%.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: flow

Use **flow** to create a flow template and enter RIR-VXLAN or RIR-SDWAN flow template view, or enter the view of an existing RIR-VXLAN or RIR-SDWAN flow template.

Use **undo flow** to delete a flow template.

Syntax

flow *flow-id*

undo flow *flow-id*

Default

No flow templates exist.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: link-select delay

Use **link-select delay** to set the link selection delay.

Use **undo link-select delay** to restore the default.

Syntax

link-select delay *delay*

undo link-select delay

Default

The link selection delay is 60 seconds.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: expect-bandwidth

Use **expect-bandwidth** to specify the per-session expected bandwidth.

Use **undo expect-bandwidth** to restore the default.

Syntax

expect-bandwidth *bandwidth*

undo expect-bandwidth

Default

The per-session expected bandwidth is 0 kbps.

Old views

RIR-VXLAN flow template view

New views

RIR-VXLAN flow template view

RIR-SDWAN flow template view

Change description

Before modification: You cannot configure this command in RIR-SDWAN flow template view.

After modification: You can configure this command in RIR-SDWAN flow template view.

Modified command: flow priority-based-schedule enable

Use **flow priority-based-schedule enable** to enable flow priority-based traffic scheduling.

Use **undo flow priority-based-schedule enable** to disable flow priority-based traffic scheduling.

Syntax

flow priority-based-schedule enable

undo flow priority-based-schedule enable

Default

Flow priority-based traffic scheduling is disabled.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: flow priority-based-schedule schedule-period

Use **flow priority-based-schedule schedule-period** to set the scheduling period for flow priority-based traffic scheduling.

Use **undo flow priority-based-schedule schedule-period** to restore the default.

Syntax

flow priority-based-schedule schedule-period *schedule-period-value*

undo flow priority-based-schedule schedule-period

Default

The scheduling period for flow priority-based traffic scheduling is 30 seconds.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: link-select suppress-period

Use **link-select suppress-period** to set the link selection suppression period.

Use **undo link-select suppress-period** to restore the default.

Syntax

link-select suppress-period *period-value*

undo link-select suppress-period

Default

No link selection suppression period is configured. The device does not start the link selection suppression period after a link selection.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: load-balance per-packet enable

Use **load-balance per-packet enable** to enable per-packet load balancing.

Use **undo load-balance enable** to restore the default.

Syntax

load-balance per-packet enable

undo load-balance enable

Default

The RIR global link load balancing mode applies.

Old views

RIR-VXLAN flow template view

New views

RIR-VXLAN flow template view

RIR-SDWAN flow template view

Change description

Before modification: You cannot configure this command in RIR-SDWAN flow template view.

After modification: You can configure this command in RIR-SDWAN flow template view.

Modified command: load-balance per-session periodic-adjust adjust-interval

Use **load-balance per-session periodic-adjust adjust-interval** to set the adjustment interval for per-session periodic link adjustment mode.

Use **undo load-balance per-session periodic-adjust adjust-interval** to restore the default.

Syntax

load-balance per-session periodic-adjust adjust-interval *interval-value*

undo load-balance per-session periodic-adjust adjust-interval

Default

The adjustment interval for per-session periodic link adjustment mode is 30 seconds.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: load-balance per-session periodic-adjust enable

Use **load-balance per-session periodic-adjust enable** to enable per-session periodic link adjustment mode.

Use **undo load-balance per-session periodic-adjust enable** to restore the default.

Syntax

load-balance per-session periodic-adjust enable

undo load-balance per-session periodic-adjust enable

Default

The per-session weight-based link selection mode is used.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: load-balance per-session periodic-adjust threshold

Use **load-balance per-session periodic-adjust threshold** to set the periodic adjustment thresholds in per-session periodic link adjustment mode.

Use **undo load-balance per-session periodic-adjust threshold** to restore the default.

Syntax

load-balance per-session periodic-adjust threshold upper *upper-threshold-value* **lower** *lower-threshold-value*

undo load-balance per-session periodic-adjust threshold

Default

The periodic adjustment upper threshold is 50% and the periodic adjustment lower threshold is 20%.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: log enable

Use **log enable** to enable RIR logging.

Use **undo log enable** to disable RIR logging.

Syntax

log enable

undo log enable

Default

RIR logging is disabled.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: jitter threshold

Use **jitter threshold** to set the link jitter threshold.

Use **undo jitter threshold** to restore the default.

Syntax

jitter threshold *threshold-value*

undo jitter threshold

Default

The link jitter threshold is 100 milliseconds.

Old views

RIR-VXLAN SLA view

New views

RIR-VXLAN SLA view

RIR-SDWAN SLA view

Change description

Before modification: You cannot configure this command in RIR-SDWAN SLA view.

After modification: You can configure this command in RIR-SDWAN SLA view.

Modified command: packet-loss threshold

Use **packet-loss threshold** to set the packet loss threshold.

Use **undo packet-loss threshold** to restore the default.

Syntax

packet-loss threshold *threshold-value*

undo packet-loss threshold

Default

The packet loss threshold is 100‰.

Old views

RIR-VXLAN SLA view

New views

RIR-VXLAN SLA view

RIR-SDWAN SLA view

Change description

Before modification: You cannot configure this command in RIR-SDWAN SLA view.

After modification: You can configure this command in RIR-SDWAN SLA view.

Modified command: probe connect

Use **probe connect** to configure NQA link connectivity probe parameters.

Use **undo probe connect** to restore the default.

Syntax

probe connect interval *interval* **timeout** *timeout*

undo probe connect

Default

For RIR-VXLAN, the NQA link connectivity probe interval is 100 milliseconds, and the timeout time is 3000 milliseconds for waiting for a response to a link connectivity probe packet.

For RIR-SDWAN, the NQA link connectivity probe interval is 1000 milliseconds, and the timeout time is 3000 milliseconds for waiting for a response to a link connectivity probe packet.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: quality-policy

Use **quality-policy** to configure a quality policy for a flow template.

Use **undo quality-policy** to restore the default.

Syntax

RIR-VXLAN:

quality-policy sla *sla-id* **nqa** *nqa-id*

undo quality-policy

RIR-SDWAN:

quality-policy sla *sla-id*

undo quality-policy

Default

No quality policy is configured for a flow template.

Old views

RIR-VXLAN flow template view

New views

RIR-VXLAN flow template view

RIR-SDWAN flow template view

Change description

Before modification: You cannot configure this command in RIR-SDWAN flow template view.

After modification: You can configure this command in RIR-SDWAN flow template view.

Modified command: sla

Use **sla** to create an SLA and enter RIR-VXLAN or RIR-SDWAN SLA view, or enter the view of an existing RIR-VXLAN or RIR-SDWAN SLA.

Use **undo sla** to delete an SLA.

Syntax

sla *sla-id*

undo sla *sla-id*

Default

No SLAs exist.

Old views

RIR-VXLAN view

New views

RIR-VXLAN view

RIR-SDWAN view

Change description

Before modification: You cannot configure this command in RIR-SDWAN view.

After modification: You can configure this command in RIR-SDWAN view.

Modified command: Enabling BFD for LSPs associated with an FEC

Feature change description

As from this version, the following features are supported when BFD control packet mode is used to detect LSPs:

- Encapsulating the LDP IPv4 Prefix FEC in MPLS echo request packets when BFD control packet mode is used to detect LSPs.
- Encapsulating the Nil FEC in MPLS echo request packets when BFD control packet mode is used to detect LSPs.

Command changes

Modified command: mpls bfd (for LSP)

Old syntax

mpls bfd *dest-addr mask-length nexthop nexthop-address* [**discriminator local** *local-id* **remote** *remote-id* [**isis-srlsp** | **ldp-lsp** | **ospf-srlsp** | **static-lsp**] | **echo**] [**template** *template-name*]

undo mpls bfd *dest-addr mask-length nexthop nexthop-address*


```
mpls bfd dest-addr mask-length [ echo ] [ template template-name ] [ backup-path  
template template-name ]
```

```
undo mpls bfd dest-addr mask-length
```

New syntax

```
mpls bfd dest-addr mask-length nexthop nexthop-address [ discriminator local local-id  
remote remote-id [ isis-srlsp | ldp-lsp | ospf-srlsp | static-lsp ] | echo | ldp-fec | nil-fec ]  
[ template template-name ]
```

```
undo mpls bfd dest-addr mask-length nexthop nexthop-address
```

```
mpls bfd dest-addr mask-length [ echo ] [ template template-name ] [ backup-path  
template template-name ]
```

```
undo mpls bfd dest-addr mask-length
```

Views

System view

Change description

The following keywords were added:

- **ldp-fec**: Encapsulates the LDP IPv4 Prefix FEC in MPLS echo request packets when BFD control packet mode is used to detect LSPs. If you do not specify this keyword, the type of the FEC carried in MPLS echo request packets is IPv4 IGP-Prefix Segment ID. The egress node of an LSP might support only the LDP IPv4 Prefix FEC. If the ingress node sends MPLS echo request packets that carry the IPv4 IGP-Prefix Segment ID type of FEC, the egress node cannot recognize this FEC type. The FEC validation on the egress node will fail and the BFD session will go down. To resolve this issue, specify the **ldp-fec** keyword to enable the ingress node to encapsulate the LDP IPv4 Prefix FEC in MPLS echo request packets. Then, FEC validation on the egress node can be successful.
- **nil-fec**: Encapsulates the Nil FEC in MPLS echo request packets when BFD control packet mode is used to detect LSPs. In LDP to SR interworking mode, the ingress node (source node) cannot determine whether the LDP LSP is connected to the SRLSP. When the ingress node uses MPLS BFD to detect LSPs, it encapsulates LDP FEC in MPLS echo request packets, which will fail the FEC type verification on the egress node (endpoint node). Then, the BFD session will go down. To resolve this issue, specify the **nil-fec** keyword to enable the ingress node to encapsulate the Nil FEC in MPLS echo request packets. The egress node will not check the FEC type of packets encapsulated with the Nil FEC.

Displaying information about specific SR-MPLS TE or SRv6 TE policies

Feature change description

As from this release, the **display bgp link-state** command supports the **color** *color-value* **end-point** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } parameter. You can specify an SR-MPLS TE or SRv6 TE policy by its color attribute and destination node.

Command changes

Modified command:display bgp link-state

Use **display bgp link-state** to display BGP LS information.

Old syntax

```
display bgp [ instance instance-name ] link-state [ ls-prefix [ advertise-info ] | peer { ipv4-address | ipv6-address } { advertised | received } [ statistics ] | statistics ]
```

New syntax

```
display bgp [ instance instance-name ] link-state [ ls-prefix [ advertise-info ] | peer { ipv4-address | ipv6-address } { advertised | received } [ statistics ] | statistics ]
```

```
display bgp [ instance instance-name ] link-state [ color color-value end-point { ipv4 ipv4-address | ipv6 ipv6-address } ]
```

Views

Any view

Change description

Before modification: This command does not support the **color** *color-value* **end-point** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } parameter.

After modification: This command supports the **color** *color-value* **end-point** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* } parameter.

Parameters

color *color-value* **end-point** { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }: Displays information about the SR-MPLS TE or SRv6 TE policy with the specified color attribute and destination node. The *color-value* argument specifies the color attribute value in the range of 0 to 4294967295. The **ipv4** *ipv4-address* option specifies a destination node by its IPv4 address. The **ipv6** *ipv6-address* option specifies a destination node by its IPv6 address.

Modified feature: Displaying session statistics for the specified flow template

Feature change description

As from this release, you can display session statistics for the specified flow template.

Command changes

Modified command: display rir sdwan session-statistics tunnel

Use **display rir sdwan session-statistics tunnel** to display service session statistics for the specified tunnel interface.

Old syntax

Centralized devices:

```
display rir sdwan session-statistics tunnel interface-number
```

Distributed devices in standalone mode: Centralized IRF devices:

```
display rir sdwan session-statistics tunnel interface-number [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display rir sdwan session-statistics tunnel interface-number [ chassis chassis-number slot slot-number ]
```

New syntax

Centralized devices:

```
display rir sdwan session-statistics tunnel interface-number [ flow flow-id ]
```

Distributed devices in standalone mode: Centralized IRF devices:

```
display rir sdwan session-statistics tunnel interface-number [ flow flow-id ] [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display rir sdwan session-statistics tunnel interface-number [ flow flow-id ] [ chassis chassis-number slot slot-number ]
```

Views

Any view

Change description

Before modification: The command does not support the **flow** *flow-id* option.

After modification: The command supports the **flow** *flow-id* option.

flow *flow-id*: Specifies a flow template by its flow ID, in the range of 1 to 65535. If you do not specify a flow ID, this command displays session statistics for all flow templates.

Modified feature: Configuring preference for a link specified by its the SDWAN tunnel group ID in the flow template

Feature change description

As from this release, when configuring a link preference for the flow template, you can specify the SDWAN tunnel group ID for the link.

Command changes

Modified command: path sdwan

Use **path sdwan** to configure a link preference for the flow template.

Use **undo path sdwan** to restore the default.

Old syntax

```
path sdwan transport-network network-name preference preference
```

```
undo path sdwan transport-network network-name
```

New syntax

```
path sdwan transport-network network-name [ group-id group-id ] preference preference  
undo path sdwan transport-network network-name [ group-id group-id ]
```

Default

No link preference is configured in a flow template.

Views

RIR-SDWAN flow template view

Change description

Before modification: The command does not support the **group-id** *group-id* option.

After modification: The command supports the **group-id** *group-id* option.

group-id *group-id*: Specifies the group ID of the SDWAN tunnel, in the range of 1 to 65535. If no SDWAN tunnel group ID is available, do not specify this option.

Modified feature: Configuring FEC optimization parameters

Feature change description

As from this release, the WAAS policy class view is added to some FEC-related commands, and the FEC optimization action is added to the WAAS policy class view of the **optimize** command.

Command changes

Modified command: fec average-ratio

Old views

WAAS policy RTP class view

New views

WAAS policy class view

WAAS policy RTP class view

Change description

Before modification: This command is not supported in WAAS policy class view.

After modification: This command is supported in WAAS policy class view.

Modified command: fec block-size

Old views

WAAS policy RTP class view

New views

WAAS policy class view

WAAS policy RTP class view

Change description

Before modification: This command is not supported in WAAS policy class view.

After modification: This command is supported in WAAS policy class view.

Modified command: fec decode-timeout

Old views

WAAS policy RTP class view

New views

WAAS policy class view

WAAS policy RTP class view

Change description

Before modification: This command is not supported in WAAS policy class view.

After modification: This command is supported in WAAS policy class view.

Modified command: fec encode-timeout

Old views

WAAS policy RTP class view

New views

WAAS policy class view

WAAS policy RTP class view

Change description

Before modification: This command is not supported in WAAS policy class view.

After modification: This command is supported in WAAS policy class view.

Modified command: match udp

Old syntax

```
match [ match-id ] udp { any | destination | source } [ ip-address ipv4-address  
[ mask-length | mask ] ]
```

```
undo match match-id
```

New syntax

```
match [ match-id ] udp any [ ip-address { ip-address [ mask-length | mask ] |  
object-group ip-object-group-name } | ipv6-address { ipv6-address [ prefix-length ] |  
object-group ipv6-object-group-name } ] [ port { port-list | object-group  
port-object-group-name } ]
```

```
match [ match-id ] udp { destination ip-address { ip-address [ mask-length | mask ] |  
object-group ip-object-group-name } } [ port { port-list | object-group  
port-object-group-name } ] | source ip-address { ip-address [ mask-length | mask ] |  
object-group ip-object-group-name } } [ port { port-list | object-group  
port-object-group-name } ] } *
```

```
match [ match-id ] udp { destination ipv6-address { ipv6-address [ prefix-length ] |
object-group ipv6-object-group-name } [ port { port-list | object-group
port-object-group-name } ] | source ipv6-address { ipv6-address [ prefix-length ] |
object-group ipv6-object-group-name } [ port { port-list | object-group
port-object-group-name } ] } *
```

```
match [ match-id ] udp { destination | source } port { port-list | object-group
port-object-group-name }
```

```
undo match match-id
```

Old views

WAAS policy RTP class view

New views

WAAS policy class view

WAAS policy RTP class view

Change description

Before modification:

- You cannot configure an IPv6 address match item or port match item for a UDP match criterion.
- You cannot configure both source and destination parameters.
- You cannot reference object groups.
- You cannot configure a UDP match criterion in WAAS policy class view.

After modification:

- You cannot configure an IPv6 address match item or port match item for a UDP match criterion.
- You cannot configure both source and destination parameters.
- You cannot reference object groups.
- You cannot configure a UDP match criterion in WAAS policy class view.

```
ip-address { ip-address [ mask-length | mask ] | object-group ip-object-group-name }:
```

Specifies IPv4 addresses for matching UDP messages.

- *ip-address*: Specifies an IPv4 address in dotted decimal notation.
- *mask-length*: Specifies the mask length for the IPv4 address, in the range of 0 to 32. The default is 32.
- *mask*: Specifies the mask for the IPv4 address. The default is 255.255.255.255.
- **object-group ip-object-group-name**: Specifies an IPv4 address object group by its name, a case-insensitive string of 1 to 63 characters.

```
ipv6-address { ipv6-address [ prefix-length ] | object-group ipv6-object-group-name }:
```

Specifies IPv6 addresses for matching UDP packets. This option is supported only in WAAS class view.

ipv6-address: Specifies an IPv6 address.

- *prefix-length*: Specifies the prefix length for the IPv6 address, in the range of 0 to 128. The default is 128.
- **object-group ipv6-object-group-name**: Specifies an IPv6 address object group by its name, a case-insensitive string of 1 to 63 characters.

```
port { port-list | object-group port-object-group-name }:
```

Specifies port numbers for matching UDP messages.

- **port port-list**: Specifies a space-separated list of up to 10 port items. Each item specifies a port number or a range of port numbers in the form of *port-number1 to port-number2*. The value for *port-number2* must be greater than or equal to the value for *port-number1*. The value range for the *port-number* argument is 1 to 65535. If you do not specify a port list, all port numbers are matched.

- **object-group** *port-object-group-name*: Specifies a port object group by its name, a case-insensitive string of 1 to 63 characters.

Modified command: optimize

Old syntax

WAAS policy class view:

```
optimize { packet-dup | tfo [ dre | lz ] * }
```

```
undo optimize
```

WAAS policy RTP class view:

```
optimize { fec | packet-dup }
```

```
undo optimize
```

New syntax

WAAS policy class view:

```
optimize { fec | packet-dup | tfo [ dre | lz ] * }
```

```
undo optimize
```

WAAS policy RTP class view:

```
optimize { fec | packet-dup }
```

```
undo optimize
```

Views

WAAS policy class view

WAAS policy RTP class view

Change description

Before modification: The FEC optimization action is not supported in WAAS policy class view.

After modification: The FEC optimization action is supported in WAAS policy class view.

Modified feature: Displaying unicast routing information generated based on the Priority-Color extended community attribute

Feature change description

As from this release, you can use the following command to view unicast routing information generated based on the Priority-Color extended community attribute:

- **display bgp routing-table ipv4 unicast**
- **display bgp routing-table ipv6 unicast**

Command changes

Modified command: display bgp routing-table ipv4 unicast

Use **display bgp routing-table ipv4 unicast** to display BGP IPv4 unicast routing information.

Old syntax

```
display bgp [ instance instance-name ] routing-table ipv4 [ unicast ] [ vpn-instance vpn-instance-name ] [ ipv4-address [ { mask-length | mask } [ longest-match ] ] | ipv4-address [ mask-length | mask ] advertise-info | as-path-acl as-path-acl-number | community-list { { basic-community-list-number | comm-list-name } [ whole-match ] | adv-community-list-number } | peer { ipv4-address | ipv6-address } { advertised-routes | received-routes } [ ipv4-address [ mask-length | mask ] | statistics ] | statistics ]
```

New syntax

```
display bgp [ instance instance-name ] routing-table ipv4 [ unicast ] [ vpn-instance vpn-instance-name ] [ ipv4-address [ { mask-length | mask } [ longest-match ] ] | ipv4-address [ mask-length | mask ] advertise-info | as-path-acl as-path-acl-number | community-list { { basic-community-list-number | comm-list-name } [ whole-match ] | adv-community-list-number } | peer { ipv4-address | ipv6-address } { advertised-routes | received-routes } [ ipv4-address [ mask-length | mask ] | statistics ] | statistics ]
```

```
display bgp [ instance instance-name ] routing-table ipv4 [ unicast ] vpn-instance vpn-instance-name system-ip
```

Views

Any view

Modified command: display bgp routing-table ipv6 unicast

Use **display bgp routing-table ipv6 unicast** to display BGP IPv6 unicast routing information.

Syntax

```
display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] [ vpn-instance vpn-instance-name ] [ ipv6-address prefix-length [ advertise-info ] | as-path-acl as-path-acl-number | community-list { { basic-community-list-number | comm-list-name } [ whole-match ] | adv-community-list-number } | peer ipv6-address { advertised-routes | received-routes } [ ipv6-address prefix-length | statistics ] | statistics ]
```

```
display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] peer ipv4-address { advertised-routes | received-routes } [ ipv6-address prefix-length | statistics ]
```

```
display bgp [ instance instance-name ] routing-table ipv6 [ unicast ] vpn-instance vpn-instance-name system-ip
```

Views

Any view

Change description

Before modification: The command does not support the **system-ip** keyword.

After modification: The command supports the **system-ip** keyword.

Parameters

system-ip: Displays IPv6 unicast routing information generated through the Priority-Color extended community attribute in the specified BGP VPN instance.

Modified feature: Specifying a TCP congestion control algorithm for the WAN side

Feature change description

As from this release, you can configure BBRv1 or BBRv2 as the TCP congestion control algorithm for the WAN side.

Command changes

Modified command: `waas tfo congestion-method`

Old syntax

```
waas tfo congestion-method { bic | reno }  
undo waas tfo congestion-method
```

New syntax

```
waas tfo congestion-method { bbrv1 | bbrv2 | bic | reno }  
undo waas tfo congestion-method
```

Views

System view

Change description

Before modification: The **bbrv1** and **bbrv2** keywords are not supported.

After modification: The **bbrv1** and **bbrv2** keywords are supported.

bbrv1: Specifies BBRv1 as the TCP congestion control algorithm.

bbrv2: Specifies BBRv2 as the TCP congestion control algorithm.

Modified feature: RIR support for VPDN links

Feature change description

As from this release, RIR supports configuring VPDN links.

Command reference

Modified command: path link-type index preference

Use **path link-type index preference** to specify a link preference for a type of links with a specific link index in a flow template.

Use **undo path link-type index preference** to restore the default.

Old syntax

```
path link-type { 4g | internet | mpls | mstp } index link-index preference preference
undo path link-type { 4g | internet | mpls | mstp } index link-index
```

New syntax

```
path link-type { 4g | internet | mpls | mstp | vpdn } index link-index preference preference
undo path link-type { 4g | internet | mpls | mstp | vpdn } index link-index
```

Default

No link preference is specified for a type of links with a specific link index in a flow template.

Views

RIR-VXLAN flow template view

Change description

Before modification: The command does not support the **vpdn** keyword.

After modification: The command supports the **vpdn** keyword.

vpdn: Specifies the VPDN type.

Modified command: rir link-type index

Use **rir link-type** to assign a link type and link index to a VSI interface.

Use **undo rir link-type** to restore the default.

Old syntax

```
rir link-type { 4g | internet | mpls | mstp } index link-index
undo rir link-type { 4g | internet | mpls | mstp } index link-index
```

New syntax

```
rir link-type { 4g | internet | mpls | mstp | vpdn } index link-index
undo rir link-type { 4g | internet | mpls | mstp | vpdn } index link-index
```

Default

No link type or link index is assigned to a VSI interface.

Views

VSI interface view

Change description

Before modification: The command does not support the **vpdn** keyword.

After modification: The command supports the **vpdn** keyword.

vpdn: Specifies the VPDN type.

Modified feature: Using the original cost of redistributed routes

Feature change description

As from this release, you can configure OSPF, IS-IS, and OSPFv3 to use the original cost of redistributed routes when enabling route redistribution.

Command changes

Modified command: import-route (OSPF view)

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Old syntax

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
import-route { direct | guard | static } [ cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
import-route eigrp [ eigrp-as | all-as ] [ allow-direct | cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
import-route { isis | ospf | rip } [ process-id | all-processes ] [ allow-direct | cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route { bgp | direct | eigrp [ eigrp-as | all-as ] | guard | { isis | ospf | rip } [ process-id | all-processes ] | static }
```

New syntax

```
import-route bgp [ as-number ] [ allow-ibgp ] [ [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
import-route { direct | guard | static } [ [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
import-route eigrp [ eigrp-as | all-as ] [ allow-direct | [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
import-route { isis | ospf | rip } [ process-id | all-processes ] [ allow-direct | [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route { bgp | direct | eigrp [ eigrp-as | all-as ] | guard | { isis | ospf | rip } [ process-id | all-processes ] | static }
```

Default

OSPF does not redistribute routes.

Views

OSPF view

Change description

Before modification: The **inherit-cost** keyword is not supported.

After modification: The **inherit-cost** keyword is supported.

Parameters

inherit-cost: Uses the original cost of redistributed routes.

Modified command: import-route (IS-IS view)

Use **import-route** to redistribute routes from another routing protocol or another IS-IS process.

Use **undo import-route** to disable route redistribution.

Old syntax

In IS-IS IPv4 unicast address family view/IS-IS IPv4 unicast topology view:

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ cost cost-value | cost-type { external | internal } ] | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] [ allow-direct | cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isis | ospf | rip } [ process-id | all-processes ] [ allow-direct | cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
undo import-route { bgp | direct | eigrp [ eigrp-as | all-as ] | { isis | ospf | rip } [ process-id | all-processes ] | static }
```

In IS-IS IPv6 unicast address family view:

```
import-route bgp4+ [ as-number ] [ allow-ibgp ] [ cost cost-value | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ cost cost-value | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isisv6 | ospfv3 | ripng } [ process-id ] [ allow-direct | cost cost-value ] | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
undo import-route { bgp4+ | direct | { isisv6 | ospfv3 | ripng } [ process-id | all-processes ] | static }
```

New syntax

In IS-IS IPv4 unicast address family view/IS-IS IPv4 unicast topology view:

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route bgp [ as-number ] [ allow-ibgp ] inherit-cost [ [ level-1 | level-1-2 | level-2 ]  
| route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ cost cost-value | cost-type { external | internal } |  
[ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } inherit-cost [ [ level-1 | level-1-2 | level-2 ] | route-policy  
route-policy-name | tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] [ allow-direct | cost cost-value | cost-type  
{ external | internal } | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name |  
tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] inherit-cost [ allow-direct | [ level-1 | level-1-2 |  
level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isis | ospf | rip } [ process-id | all-processes ] [ allow-direct | cost  
cost-value | cost-type { external | internal } | [ level-1 | level-1-2 | level-2 ] |  
route-policy route-policy-name | tag tag ] *
```

```
import-route { isis | ospf | rip } [ process-id | all-processes ] inherit-cost [ allow-direct  
| [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
undo import-route { bgp | direct | eigrp [ eigrp-as | all-as ] | { isis | ospf | rip }  
[ process-id | all-processes ] | static }
```

In IS-IS IPv6 unicast address family view:

```
import-route bgp4+ [ as-number ] [ allow-ibgp ] [ [ cost cost-value | inherit-cost ] |  
[ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ [ cost cost-value | inherit-cost ] | [ level-1 | level-1-2 |  
level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isisv6 | ospfv3 | ripng } [ process-id ] [ allow-direct | [ cost cost-value |  
inherit-cost ] ] | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ]  
*
```

```
undo import-route { bgp4+ | direct | { isisv6 | ospfv3 | ripng } [ process-id |  
all-processes ] | static }
```

Default

IS-IS does not redistribute routes from other routing protocols or processes.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv4 unicast topology view

IS-IS IPv6 unicast address family view

Change description

Before modification: The **inherit-cost** keyword is not supported.

After modification: The **inherit-cost** keyword is supported.

Parameters

inherit-cost: Uses the original cost of redistributed routes.

Modified command: import-route (OSPFv3 view)

Use **import-route** to enable route redistribution.

Use **undo import-route** to disable route redistribution.

Old syntax

```
import-route bgp4+ [ as-number ] [ allow-ibgp ] [ cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route bgp4+
```

```
import-route { direct | guard | static } [ cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route { direct | guard | static }
```

```
import-route { isisv6 | ospfv3 | ripng } [ process-id | all-processes ] [ allow-direct | cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route { isisv6 | ospfv3 | ripng } [ process-id | all-processes ]
```

New syntax

```
import-route bgp4+ [ as-number ] [ allow-ibgp ] [ [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route bgp4+
```

```
import-route { direct | guard | static } [ [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route { direct | guard | static }
```

```
import-route { isisv6 | ospfv3 | ripng } [ process-id | all-processes ] [ allow-direct | [ cost cost-value | inherit-cost ] | nssa-only | route-policy route-policy-name | tag tag | type type ] *
```

```
undo import-route { isisv6 | ospfv3 | ripng } [ process-id | all-processes ]
```

Default

OSPFv3 does not redistribute routes.

Views

OSPFv3 view

Change description

Before modification: The **inherit-cost** keyword is not supported.

After modification: The **inherit-cost** keyword is supported.

Parameters

inherit-cost: Uses the original cost of redistributed routes.

Modified feature: Configuring IS-IS to redistribute user network routes and

redistribute routes without keeping their SR labels

Feature change description

As from this release, you can configure IS-IS to redistribute user network routes and redistribute routes without keeping their SR labels.

Command changes

Modified command: import-route

Use **import-route** to redistribute routes from another routing protocol or another IS-IS process.

Use **undo import-route** to disable route redistribution.

Old syntax

In IS-IS IPv4 unicast address family view/IS-IS IPv4 unicast topology view:

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] [ route-policy route-policy-name | tag tag ] *
```

```
import-route bgp [ as-number ] [ allow-ibgp ] inherit-cost [ [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] [ route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } inherit-cost [ [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] [ allow-direct | cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] [ route-policy route-policy-name | tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] inherit-cost [ allow-direct | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route rip [ process-id | all-processes ] [ allow-direct | cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] [ route-policy route-policy-name | tag tag ] *
```

```
import-route rip [ process-id | all-processes ] inherit-cost [ allow-direct | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isis | ospf } [ process-id | all-processes ] [ allow-direct | cost cost-value | cost-type { external | internal } ] [ level-1 | level-1-2 | level-2 ] [ route-policy route-policy-name | tag tag ] *
```

```
import-route { isis | ospf } [ process-id | all-processes ] inherit-cost [ allow-direct | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
undo import-route { bgp | direct | eigrp [ eigrp-as | all-as ] | { isis | ospf | rip } [ process-id | all-processes ] | static }
```

In IS-IS IPv6 unicast address family view:

```
import-route bgp4+ [ as-number ] [ allow-ibgp ] [ [ cost cost-value | inherit-cost ] |  
[ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ [ cost cost-value | inherit-cost ] | [ level-1 | level-1-2 |  
level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isisv6 | ospfv3 | ripng } [ process-id ] [ allow-direct | [ cost cost-value |  
inherit-cost ] | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ]  
*
```

```
undo import-route { bgp4+ | direct | { isisv6 | ospfv3 | ripng } [ process-id ] | static }
```

New syntax

In IS-IS IPv4 unicast address family view/IS-IS IPv4 unicast topology view:

```
import-route bgp [ as-number ] [ allow-ibgp ] [ cost cost-value | cost-type { external |  
internal } | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route bgp [ as-number ] [ allow-ibgp ] inherit-cost [ [ level-1 | level-1-2 | level-2 ] |  
route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static | unr } [ cost cost-value | cost-type { external | internal } |  
[ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static | unr } inherit-cost [ [ level-1 | level-1-2 | level-2 ] |  
route-policy route-policy-name | tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] [ allow-direct | cost cost-value | cost-type  
{ external | internal } | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name |  
tag tag ] *
```

```
import-route eigrp [ eigrp-as | all-as ] inherit-cost [ allow-direct | [ level-1 | level-1-2 |  
level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route rip [ process-id | all-processes ] [ allow-direct | cost cost-value | cost-type  
{ external | internal } | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name |  
tag tag ] *
```

```
import-route rip [ process-id | all-processes ] inherit-cost [ allow-direct | [ level-1 |  
level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { isis | ospf } [ process-id | all-processes ] [ allow-direct | cost cost-value |  
cost-type { external | internal } | [ level-1 | level-1-2 | level-2 ] | no-sid | route-policy  
route-policy-name | tag tag ] *
```

```
import-route { isis | ospf } [ process-id | all-processes ] inherit-cost [ allow-direct |  
[ level-1 | level-1-2 | level-2 ] | no-sid | route-policy route-policy-name | tag tag ] *
```

```
undo import-route { bgp | direct | eigrp [ eigrp-as | all-as ] | { isis | ospf | rip }  
[ process-id | all-processes ] | static | unr }
```

In IS-IS IPv6 unicast address family view:

```
import-route bgp4+ [ as-number ] [ allow-ibgp ] [ [ cost cost-value | inherit-cost ] |  
[ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ] *
```

```
import-route { direct | static } [ [ cost cost-value | inherit-cost ] | [ level-1 | level-1-2 |  
level-2 ] | route-policy route-policy-name | tag tag ] *
```



```
import-route { isisv6 | ospfv3 | ripng } [ process-id ] [ allow-direct | [ cost cost-value |
inherit-cost ] | [ level-1 | level-1-2 | level-2 ] | route-policy route-policy-name | tag tag ]
*
```

```
undo import-route { bgp4+ | direct | { isisv6 | ospfv3 | ripng } [ process-id ] | static }
```

Default

IS-IS does not redistribute routes from other routing protocols or processes.

Views

IS-IS IPv4 unicast address family view

IS-IS IPv4 unicast topology view

IS-IS IPv6 unicast address family view

Change description

Before modification: The **unr** and **no-sid** keywords are not supported.

After modification: The **unr** and **no-sid** keywords are supported.

Parameters

unr: Redistributes user network routes. User network routes are generated by access devices for online users.

no-sid: Redistributes routes without keeping their SR labels. If you do not specify this keyword, IS-IS redistributes routes without removing their SR labels.

Modified feature: Setting the speed of an Ethernet interface

Feature change description

As from this release, the device provides 25GBASE-R-SFP28 Ethernet interfaces. You can use the **speed** command to set the speed of a 25G interface to match the rate of a transceiver module.

Command changes

Modified command: speed

Old syntax

```
speed { 10 | 100 | 1000 | 10000 | auto }
```

```
undo speed
```

New syntax

```
speed { 10 | 100 | 1000 | 10000 | 25000 | auto }
```

```
undo speed
```

Views

Ethernet interface view

Change description

The device provides 25GBASE-R-SFP28 Ethernet interfaces. The **25000** keyword was added to the **speed** command for you to set the speed of a 25GBASE-R-SFP28 Ethernet interface on an SPU-300-G to match the rate of the transceiver module.

Modified feature: Configuring load sharing for link aggregation groups based on flow labels

Feature change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Command changes

Modified command:

Old syntax

```
link-aggregation global load-sharing mode { { destination-ip | destination-mac |  
destination-port | source-ip | source-mac | source-port } * per-packet }  
undo link-aggregation global load-sharing mode
```

New syntax

```
link-aggregation global load-sharing mode { { destination-ip | destination-mac |  
destination-port | flow-label | source-ip | source-mac | source-port } * per-packet }  
undo link-aggregation global load-sharing mode
```

Views

System view

Change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Modified command:

Old syntax

```
link-aggregation load-sharing mode { { destination-ip | destination-port | ip-protocol |  
mpls-label1 | mpls-label2 | mpls-label3 | source-ip | source-port } * | bandwidth-usage  
| per-packet }  
undo link-aggregation load-sharing mode
```

New syntax

```
link-aggregation load-sharing mode { { destination-ip | destination-port | flow-label |  
ip-protocol | mpls-label1 | mpls-label2 | mpls-label3 | source-ip | source-port } * |  
bandwidth-usage | per-packet }
```

```
undo link-aggregation load-sharing mode
```

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Modified command:

Old syntax

```
link-aggregation global load-sharing mode { destination-ip | destination-mac |  
destination-port | mpls-label1 | source-ip | source-mac | source-port } *
```

```
undo link-aggregation global load-sharing mode
```

New syntax

```
link-aggregation global load-sharing mode { destination-ip | destination-mac |  
destination-port | flow-label | mpls-label1 | source-ip | source-mac | source-port } *
```

```
undo link-aggregation global load-sharing mode
```

Views

System view

Change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Modified command:

Old syntax

```
link-aggregation load-sharing mode { { destination-ip | destination-port | source-ip |  
source-port } * | bandwidth-usage | per-packet }
```

```
undo link-aggregation load-sharing mode
```

New syntax

```
link-aggregation load-sharing mode { { destination-ip | destination-port | flow-label |  
source-ip | source-port } * | bandwidth-usage | per-packet }
```

```
undo link-aggregation load-sharing mode
```

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Modified command: link-aggregation global load-sharing mode

Old syntax

```
link-aggregation global load-sharing mode { destination-ip | destination-mac |  
destination-port | mpls-label1 | source-ip | source-mac | source-port } *  
undo link-aggregation global load-sharing mode
```

New syntax

```
link-aggregation global load-sharing mode { destination-ip | destination-mac |  
destination-port | flow-label | mpls-label1 | source-ip | source-mac | source-port } *  
undo link-aggregation global load-sharing mode
```

Views

System view

Change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Modified command: link-aggregation load-sharing mode

Old syntax

```
link-aggregation load-sharing mode { { destination-ip | destination-port | source-ip |  
source-port } * | bandwidth-usage | per-packet }  
undo link-aggregation load-sharing mode
```

New syntax

```
link-aggregation load-sharing mode { { destination-ip | destination-port | flow-label |  
source-ip | source-port } * | bandwidth-usage | per-packet }  
undo link-aggregation load-sharing mode
```

Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

Change description

Use the **flow-label** keyword to configure load sharing for link aggregation groups based on flow labels.

Modified feature: QinQ support for new views and keywords

Feature change description

As from this release, you can enable QinQ in VEB interface view on a device.

As from this release, the **dot1ad** and **dot1q** keywords were added to the **qinq ethernet-type** command. The **dot1ad** keyword sets the hexadecimal TPID value to 88a8. The **dot1q** keyword sets the hexadecimal TPID value to 8100.

Command changes

Modified command: qinq enable

Syntax

```
qinq enable
undo qinq enable
```

Views

Layer 2 Ethernet interface view

Change description

Before modification: The **qinq enable** command is supported only in Layer 2 Ethernet interface view.

After modification: The **qinq enable** command is supported in Layer 2 Ethernet interface view and VEB interface view.

Modified command: qinq ethernet-type (interface view)

Old syntax

```
qinq ethernet-type service-tag hex-value
undo qinq ethernet-type service-tag
```

New syntax

```
qinq ethernet-type service-tag { hex-value | dot1ad | dot1q }
undo qinq ethernet-type service-tag
```

Views

Layer 2 Ethernet interface view

Change description

Before modification: The **qinq enable** command is supported only in Layer 2 Ethernet interface view.

After modification: The **qinq enable** command is supported in Layer 2 Ethernet interface view and VEB interface view. The **dot1ad** keyword is added to set the hexadecimal TPID value to 88a8. The **dot1q** keyword is added to set the hexadecimal TPID value to 8100.

Modified command: qinq ethernet-type (system view)

Old syntax

```
qinq ethernet-type customer-tag hex-value
```

```
undo qinq ethernet-type customer-tag
```

New syntax

```
qinq ethernet-type customer-tag { hex-value | dot1ad | dot1q }
```

```
undo qinq ethernet-type customer-tag
```

Views

System view

Change description

After modification: The **dot1ad** and **dot1q** keywords are added to the command.

- The **dot1ad** keyword sets the hexadecimal TPID value to 88a8.
- The **dot1q** keyword sets the hexadecimal TPID value to 8100.

Modified feature: QinQ support for new keywords

Feature change description

As from this release, the **dot1ad** and **dot1q** keywords were added to the **qinq ethernet-type** command. The **dot1ad** keyword sets the hexadecimal TPID value to 88a8. The **dot1q** keyword sets the hexadecimal TPID value to 8100.

Command changes

Modified command: qinq ethernet-type (interface view)

Old syntax

```
qinq ethernet-type service-tag hex-value
```

```
undo qinq ethernet-type service-tag
```

New syntax

```
qinq ethernet-type service-tag { hex-value | dot1ad | dot1q }
```

```
undo qinq ethernet-type service-tag
```

Views

Layer 2 Ethernet interface view

Change description

After modification: The **dot1ad** and **dot1q** keywords are added to the command.

- The **dot1ad** keyword sets the hexadecimal TPID value to 88a8.
- The **dot1q** keyword sets the hexadecimal TPID value to 8100.

Modified command: qinq ethernet-type (system view)

Old syntax

```
qinq ethernet-type customer-tag hex-value  
undo qinq ethernet-type customer-tag
```

New syntax

```
qinq ethernet-type customer-tag { hex-value | dot1ad | dot1q }  
undo qinq ethernet-type customer-tag
```

Views

System view

Change description

After modification: The **dot1ad** and **dot1q** keywords are added to the command.

- The **dot1ad** keyword sets the hexadecimal TPID value to 88a8.
- The **dot1q** keyword sets the hexadecimal TPID value to 8100.

Modified feature: Recursing an IPv6 static route to the specified SRv6 TE policy

Feature change description

As from this release, you can recurse an IPv6 static route to the specified SRv6 TE policy.

Command changes

Modified command: ipv6 route-static

Old syntax

N/A

New syntax

```
ipv6 route-static ipv6-address prefix-length srv6-policy { color color-value end-point ipv6  
ipv6-address | name policy-name } [ sid sid ] [ preference preference ] [ tag tag-value ]  
[ description text ]
```

```
undo ipv6 route-static ipv6-address prefix-length [ srv6-policy { color color-value  
end-point ipv6 ipv6-address | name policy-name } ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length srv6-policy  
{ color color-value end-point ipv6 ipv6-address | name policy-name } [ sid sid ]  
[ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length  
[ srv6-policy { color color-value end-point ipv6 ipv6-address | name policy-name } ]
```

Views

System view

Parameters

The following parameters are newly added:

- **srv6-policy name** *policy-name*: Specifies an SRv6 TE policy by its name for IPv6 static route recursion. The *policy-name* argument represents the SRv6 TE policy name, a case-sensitive string of 1 to 59 characters.
- **srv6-policy color** *color-value* **end-point ipv6** *ipv6-address*: Specifies an SRv6 TE policy by its color and endpoint attributes for IPv6 static route recursion. The *color-value* argument represents the color attribute value of the SRv6 TE policy, in the range of 0 to 4294967295. The *ipv6-address* argument represents the endpoint IPv6 address of the SRv6 TE policy.
- **sid** *sid*: Specifies the SRv6 SID of the endpoint. Packets forwarded through the SRv6 TE policy will be further forwarded based on the SRv6 SID.

Modified feature: Recursing a static route to the specified SRv6 TE policy

Feature change description

As from this release, you can recurse a static route to the specified SRv6 TE policy.

Command changes

Modified command: ip route-static and ip route-static vpn-instance

Old syntax

N/A

New syntax

```
ip route-static dest-address { mask-length | mask } { srv6-policy { color color-value end-point ipv6 ipv6-address | name policy-name } } [ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ip route-static dest-address { mask-length | mask } [ srv6-policy { name policy-name | color color-value end-point ipv6 ipv6-address } ]
```

```
ip route-static vpn-instance s-vpn-instance-name dest-address { mask-length | mask } { srv6-policy { color color-value end-point ipv6 ipv6-address | name policy-name } } [ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ip route-static vpn-instance s-vpn-instance-name dest-address { mask-length | mask } [ srv6-policy { color color-value end-point ipv6 ipv6-address | name policy-name } ]
```

Views

System view

Parameters

The following parameters are newly added:

- **srv6-policy name** *policy-name*: Specifies an SRv6 TE policy by its name for static route recursion. The *policy-name* argument represents the SRv6 TE policy name, a case-sensitive string of 1 to 59 characters.
- **srv6-policy color** *color-value* **end-point ipv6** *ipv6-address*: Specifies an SRv6 TE policy by its color and endpoint attributes for static route recursion. The *color-value* argument represents the color attribute value of the SRv6 TE policy, in the range of 0 to 4294967295. The *ipv6-address* argument represents the endpoint IPv6 address of the SRv6 TE policy.

Modified feature: Support for specifying a BJCA server for an AAA private-protocol scheme

Feature change description

Added the **bjca-auth-server** keyword to the **authentication-server** command for users to specify a BJCA server for an AAA private-protocol scheme.

Command changes

Modified command: authentication-server

Old syntax

```
authentication-server jit-auth-server
undo authentication-server jit-auth-server
```

New syntax

```
authentication-server { bjca-auth-server | jit-auth-server } auth-server-name
undo authentication-server { bjca-auth-server | jit-auth-server }
```

Views

AAA private protocol scheme view

Change description

Added the following keywords:

bjca-auth-server: Specifies a BJCA server.

Modified feature: Support of configuring an AAA private protocol scheme for IKE extended authentication

Feature change description

The **aaa-private-protocol-scheme** *aaa-private-protocol-scheme-name* option was added to the **authorization ike** command for users to specifying an AAA private protocol scheme for IKE extended authentication.

Command changes

Modified command: **authorization ike**

Old syntax

```
authorization ike { local [ radius-scheme radius-scheme-name ] [ none ] | none |  
radius-scheme radius-scheme-name [ local ] [ none ] }  
undo authorization ike
```

New syntax

```
authorization ike { aaa-private-protocol-scheme aaa-private-protocol-scheme-name |  
local [ radius-scheme radius-scheme-name ] [ none ] | none | radius-scheme  
radius-scheme-name [ local ] [ none ] }  
undo authorization ike
```

Views

ISP domain view

Change description

Added the following keywords:

aaa-private-protocol-scheme *aaa-private-protocol-scheme-name*: Specifies an AAA private protocol scheme by its name, a case-insensitive string of 1 to 32 characters.

Modified feature: Support of displaying IPv4 unicast routing information generated based on the Priority-Color extended community attribute for a BGP-VPN instance routing table

Feature change description

As from this release, you can use the **display bgp routing-table vpnv4** command to display IPv4 unicast routing information generated based on the Priority-Color extended community attribute for a BGP-VPN instance routing table.

Command changes

Modified command: **display bgp routing-table vpnv4**

New syntax

display bgp [**instance** *instance-name*] **routing-table vpnv4 system-ip**

Views

Any view

Change description

Before modification: The command does not support the **system-ip** keyword.

After modification: The command supports the **system-ip** keyword.

Parameters

system-ip: Displays IPv4 unicast routing information generated through the Priority-Color extended community attribute in the specified BGP VPN instance.

Modified feature: Configuring the parameters carried in the URL of a portal Web server

Feature change description

As from this release, the device supports configuring the BAS-IP attribute of portal packets as a parameter to be carried in the URL of a portal Web server. The access device will redirect a portal user by sending the URL with the BAS-IP attribute parameter to the user.

Command changes

Modified command: url-parameter

Old syntax

```
url-parameter param-name { nas-id | nas-port-id | original-url | source-address | ssid |  
{ ap-mac | low-mac | source-mac } [ format section { 1 | 3 | 6 } { lowercase |  
uppercase } ] [ encryption { aes | des } key { cipher | simple } string ] | value  
expression | vlan }
```

New syntax

```
url-parameter param-name { bas-ip | nas-id | nas-port-id | original-url | source-address  
| ssid | { ap-mac | low-mac | source-mac } [ format section { 1 | 3 | 6 } { lowercase |  
uppercase } ] [ encryption { aes | des } key { cipher | simple } string ] | value  
expression | vlan }
```

Views

Portal Web server view

Change description

The **bas-ip** keyword is added to the command to specify the BAS-IP attribute of portal packets.

Modified feature: Change of default values for the single-hop BFD detection time multiplier and SBFD detection time multiplier

Feature change description

As from this release, the default values of the single-hop BFD detection time multiplier and SBFD detection time multiplier are changed.

Command changes

Modified command: bfd detect-multiplier (BFD)

Use **bfd detect-multiplier** to set the single-hop BFD detection time multiplier for control packet mode and echo packet mode.

Use **undo bfd detect-multiplier** to restore the default.

Syntax

```
bfd detect-multiplier value
```

```
undo bfd detect-multiplier
```

Views

Interface view
BFD template view
Static BFD session view

Change description

Before modification: By default, the single-hop BFD detection time multiplier is 5.
After modification: By default, the single-hop BFD detection time multiplier is 3.

Modified command: bfd detect-multiplier (SBFD)

Use **bfd detect-multiplier** to set the SBFD detection time multiplier in BFD template view.
Use **undo bfd detect-multiplier** to restore the default.

Syntax

bfd detect-multiplier *value*
undo bfd detect-multiplier

Views

BFD template view

Change description

Before modification: By default, the SBFD detection time multiplier is 5.
After modification: By default, the SBFD detection time multiplier is 3.

Modified feature: Displaying VRRP version information in the output from the display vrrp command

Feature change description

As from this release, the output from the **display vrrp** command displays VRRP version information.

Command changes

Modified command: display vrrp

Use **display vrrp** to display the states of IPv4 VRRP groups.

Syntax

display vrrp [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]
[**verbose**]

Views

Any view

Change description

Before modification: The VRRP version information is not displayed in the command output.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
  RBM control channel is established
  VRRP active group status: Master
  VRRP standby group status: Backup
Total number of virtual routers : 3
Interface GigabitEthernet1/0/1
  VRID              : 1                      Adver Timer   : 100
  Admin Status      : Up                    State         : Master
  Config Pri        : 150                   Running Pri    : 150
  Preempt Mode      : Yes                   Delay Time    : 5
  Auth Type         : Simple                 Key           : *****
  Virtual IP        : 1.1.1.1
  Virtual MAC       : 0000-5e00-0101
  Master IP         : 1.1.1.2
```

After modification: The VRRP version information is displayed in the command output.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
  Running Mode      : Standard
  RBM control channel is established
  VRRP active group status: Master
  VRRP standby group status: Backup
Total number of virtual routers : 3
Interface GigabitEthernet1/0/1
  VRID              : 1                      Adver Timer   : 100
  Admin Status      : Up                    State         : Master
  Config Pri        : 150                   Running Pri    : 150
  Preempt Mode      : Yes                   Delay Time    : 5
  Auth Type         : Simple                 Key           : *****
  Version           : 2
  Virtual IP        : 1.1.1.1
  Virtual MAC       : 0000-5e00-0101
  Master IP         : 1.1.1.2
```

Modified feature: Configuring the parameters carried in the URL of a portal Web server

Feature change description

As from this release, the device supports configuring the BAS-IP attribute of portal packets as a parameter to be carried in the URL of a portal Web server. After you configure the BAS-IP attribute,

the access device redirects a portal user by sending the URL with the BAS-IP attribute parameter to the user.

Command changes

Modified command: url-parameter

Old syntax

```
url-parameter param-name { nas-id | nas-port-id | original-url | source-address | ssid |  
{ ap-mac | low-mac | source-mac } [ format section { 1 | 3 | 6 } { lowercase |  
uppercase } ] [ encryption { aes | des } key { cipher | simple } string ] | value  
expression | vlan }
```

New syntax

```
url-parameter param-name { bas-ip | nas-id | nas-port-id | original-url | source-address  
| ssid | { ap-mac | low-mac | source-mac } [ format section { 1 | 3 | 6 } { lowercase |  
uppercase } ] [ encryption { aes | des } key { cipher | simple } string ] | value  
expression | vlan }
```

Views

Portal Web server view

Change description

The **bas-ip** keyword is added to the command to specify the BAS-IP attribute of portal packets.

Modified command: display portal web-server

Syntax

```
display portal web-server [ server-name ]
```

Views

Any view

Change description

Before modification: The BAS-IP attribute carried in the URL of a portal Web server was not displayed in the output for this command.

```
<Sysname> display portal web-server wbs  
Portal Web server: wbs  
Type: IMC  
URL: http://www.test.com/portal  
URL parameters:  
    userip=source-address  
VPN instance: Not configured  
Server detection:  
    Interval: 120s  
    Attempts: 5  
    Action: log, trap  
    Detection URL: http://www.test.com/portal  
    Detection type: TCP  
IPv4 status: Up
```

```

IPv6 status: Up
Captive-bypass: Disabled
If-match: original-url: http://2.2.2.2, redirect-url: http://192.168.56.2
          original-url: http://1.1.1.1, temp-pass redirect-url:
          http://192.168.1.1

# After modification: The BAS-IP attribute carried in the URL of a portal Web server is displayed in
the output for this command.
<Sysname> display portal web-server wbs
Portal Web server: wbs
  Type: IMC
  URL: http://www.test.com/portal
  URL parameters:
    basip=bas-ip
    userip=source-address
  VPN instance: Not configured
  Server detection:
    Interval: 120s
    Attempts: 5
    Action: log, trap
    Detection URL: http://www.test.com/portal
    Detection type: TCP
  IPv4 status: Up
  IPv6 status: Up
  Captive-bypass: Disabled
  If-match: original-url: http://2.2.2.2, redirect-url: http://192.168.56.2
            original-url: http://1.1.1.1, temp-pass redirect-url:
            http://192.168.1.1

```

Modified feature: Using the gateway IP address obtained from the DHCP server through the specified interface as the next hop IP address for probe packets

Feature change description

As from this release, you can configure NQA to use the gateway IP address obtained from the DHCP server through the interface specified in the **out interface** command as the next hop IP address for probe packets

Command changes

Modified command: next-hop

Old syntax

next-hop ip *ip-address*

next-hop ipv6 *ipv6-address*

New syntax

next-hop { dhcp | ip *ipv4-address* **| ipv6** *ipv6-address* **}**

Views

ICMP echo operation view

DNS/ICMP/TCP half open template view

Change description

Before modification: The **dhcp** keyword is not supported.

After modification: The **dhcp** keyword is supported.

dhcp: Uses the gateway IP address obtained from the DHCP server through the interface specified in the **out interface** command as the next hop IP address for probe packets. When you specify this keyword, you must also configure the **out interface** command. This keyword is supported only in ICMP echo operation view.

Modified feature: Specifying the aging parameters for dynamic flows

Feature change description

As from this release, iFIT supports specifying an aging threshold in percentage for dynamic flows.

Command changes

Modified command: dynamic-flow aging-time

Old syntax

dynamic-flow aging-time *multi-value*

New syntax

dynamic-flow aging-time *multi-value* [**threshold-percent** *threshold-percent*]

Views

iFIT view

Change description

The **threshold-percent** *threshold-percent* option is added:

threshold-percent *threshold-percent*: Specifies an aging threshold in percentage, in the range of 0 to 100. The default is 0.

Modified feature: Specifying the measurement period for an iFIT instance

Feature change description

As from this release, the device does not support setting the measurement period for an iFIT instance to one second.

Command changes

Modified command: period

Syntax

period *period*

undo period

Views

iFIT instance view

Change description

Before modification: *period*: Specifies the measurement period for an iFIT instance. Valid values include 1, 10, 30, 60, and 300, in seconds.

After modification: *period*: Specifies the measurement period for an iFIT instance. Valid values include 10, 30, 60, and 300, in seconds.

Modified feature: Binding additional analyzers to a collector instance

Feature change description

As from this release, you can bind additional analyzers to a collector instance.

Command changes

Modified command: analyzer

Old syntax

analyzer *analyzer-id* [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*]

New syntax

```
analyzer analyzer-id [ udp-port port-number ] [ vpn-instance vpn-instance-name ]  
[ additional ]
```

Views

Collector view

Collector instance view

Change description

Before modification: The **additional** keyword is not supported.

After modification: The **additional** keyword is supported.

additional: Specifies the analyzer as an additional analyzer.

Modified feature: Binding an MP to an interface

Feature change description

As from this release, you can execute the **inqa mp** command in VSI interface view and VSI subinterface view.

Command changes

Modified command: inqa mp

Syntax

```
inqa mp mp-id
```

```
undo inqa mp
```

Old views

Ethernet interface view

Aggregate interface view

New views

Ethernet interface view

Aggregate interface view

VSI interface view

VSI subinterface view

Change description

Before modification: The **inqa mp** command is not supported in VSI interface view or VSI subinterface view.

After modification: The **inqa mp** command is supported in VSI interface view and VSI subinterface view.

Modified feature: Specifying the length of probe packets for a tracer operation

Feature change description

As from this release, you can specify the length of probe packets to trace the path that the IPv4 packets traverse from source to destination.

Command changes

Modified command: tracer

Old syntax

```
tracer [ -a source-ip | -f first-ttl | -i interface-type interface-number | -m max-ttl | -p port | -q packet-number | -t tos | { -topology topo-name | -vpn-instance vpn-instance-name | -resolve-as { global | none | vpn } ] | -w timeout ] * host
```

New syntax

```
tracer [ -a source-ip | -f first-ttl | -i interface-type interface-number | -m max-ttl | -p port | -q packet-number | -s packet-size | -t tos | { -topology topo-name | -vpn-instance vpn-instance-name | -resolve-as { global | none | vpn } ] | -w timeout ] * host
```

Views

Any view

Change description

The **-s** *packet-size* option is added to this command.

-s *packet-size*: Specifies the length (in bytes) of probe packets. The value range for the *packet-size* argument is 12 to 9600. The default setting is 12 bytes.

Modified feature: Specifying the source IPv6 address of the probe packets for an IPv6 tracer operation

Feature change description

As from this release, you can specify the source IPv6 address of the probe packets to trace the path that the IPv6 packets traverse from source to destination.

Command changes

Modified command: `tracert ipv6`

Old syntax

```
tracert ipv6 [ -f first-hop | -i interface-type interface-number | -m max-hops | -p port | -q packet-number | -t traffic-class | -vpn-instance vpn-instance-name [ -resolve-as { global | none | vpn } ] | -w timeout ] * host
```

New syntax

```
tracert ipv6 [ -a source-ipv6 | -f first-hop | -i interface-type interface-number | -m max-hops | -p port | -q packet-number | -t traffic-class | -vpn-instance vpn-instance-name [ -resolve-as { global | none | vpn } ] | -w timeout ] * host
```

Views

Any view

Change description

The **-a** *source-ipv6* option is added to this command.

-a *source-ipv6*: Specifies a valid IPv6 address on the device as the source IPv6 address of the probe packets. If you do not specify a source IPv6 address, the source IPv6 address of the probe packets is the IPv6 address of the outbound interface. For information about the address selection rule, see RFC 3484.

Modified feature: Setting the flow log version

Feature change description

As from this release, the device supports setting the flow log version to 7.0.

Command changes

Modified command: `userlog flow export version`

Syntax

```
userlog flow export version version-number  
undo userlog flow export version
```

Views

System view

Change description

Before modification: The options for the *version-number* argument are 1, 3, and 5, which represent version 1.0, version 3.0, and version 5.0, respectively.

After modification: The options for the *version-number* argument are 1, 3, 5, and 7, which represent version 1.0, version 3.0, version 5.0, and version 7.0, respectively.

Modified feature: Filtering the output from a display command with a regular expression

Feature change description

As from this release, the device supports displays the number of all lines when you filter in the output from a **display** command with a regular expression.

Command changes

Modified command: `display | { begin | exclude | include }`

Old syntax

`display command | { begin | exclude | include } regular-expression`

New syntax

`display command [| { count | { begin | exclude | include } regular-expression }]
&<1-128>`

Views

Any view

Change description

The following are added:

count: Displays the number of all lines in the output from a **display** command.

&<1-128>: Specifies a maximum of 128 filter conditions.

Modified feature: Configuring the NAT device to ignore the protocol packet type

Feature change description

As from this release, you can configure the device to ignore the protocol packet type when TCP, ICMP, or SCTP packet exchanges trigger the creation of session entries.

Command changes

Modified command: `display nat all`

Syntax

`display nat all`

Views

Any view

Change description

The **Packet type ignore** field is added to the command output.

- If this field displays **Y**, the NAT device does not check the protocol packet type.
- If this field is not displayed, the NAT device checks the protocol packet type.

Modified command: display nat static

Syntax

display nat static

Views

Any view

Change description

The **Packet type ignore** field is added to the command output.

- If this field displays **Y**, the NAT device does not check the protocol packet type.
- If this field is not displayed, the NAT device checks the protocol packet type.

Modified command: nat static inbound

Old syntax

```
nat static inbound global-ip [ vpn-instance global-vpn-instance-name ] local-ip  
[ vpn-instance local-vpn-instance-name ] [ acl { ipv4-acl-number | name ipv4-acl-name }  
[ reversible ] ] [ rule rule-name ] [ priority priority ] [ disable ] [ counting ]  
[ description text ]
```

```
undo nat static inbound global-ip [ vpn-instance global-vpn-instance-name ] local-ip  
[ vpn-instance local-vpn-instance-name ]
```

New syntax

```
nat static inbound global-ip [ vpn-instance global-vpn-instance-name ] local-ip  
[ vpn-instance local-vpn-instance-name ] [ acl { ipv4-acl-number | name ipv4-acl-name }  
[ reversible ] ] [ rule rule-name ] [ priority priority ] [ disable ] [ counting ]  
[ packet-type-ignore ] [ description text ]
```

```
undo nat static inbound global-ip [ vpn-instance global-vpn-instance-name ] local-ip  
[ vpn-instance local-vpn-instance-name ]
```

Views

Any view

Change description

The **packet-type-ignore** keyword is added.

packet-type-ignore: Ignores the protocol packet type when the device creates session entries for TCP, ICMP, or SCTP. If you do not specify this keyword, the NAT device checks the protocol packet type and creates session entries for only protocol packets that pass the check. For example, the NAT device creates session entries for TCP packets only when the packet type is SYN or ACK.

Modified command: nat static outbound

Old syntax

```
nat static outbound local-ip [ vpn-instance local-vpn-instance-name ] global-ip  
[ vpn-instance global-vpn-instance-name ] [ acl { ipv4-acl-number | name ipv4-acl-name }  
[ reversible ] ] [ vrrp virtual-router-id ] [ rule rule-name ] [ priority priority ] [ disable ]  
[ counting ] [ description text ]  
  
undo nat static outbound local-ip [ vpn-instance local-vpn-instance-name ] global-ip  
[ vpn-instance global-vpn-instance-name ]
```

New syntax

```
nat static outbound local-ip [ vpn-instance local-vpn-instance-name ] global-ip  
[ vpn-instance global-vpn-instance-name ] [ acl { ipv4-acl-number | name ipv4-acl-name }  
[ reversible ] ] [ vrrp virtual-router-id ] [ rule rule-name ] [ priority priority ] [ disable ]  
[ counting ] [ packet-type-ignore ] [ description text ]  
  
undo nat static outbound local-ip [ vpn-instance local-vpn-instance-name ] global-ip  
[ vpn-instance global-vpn-instance-name ]
```

Views

Any view

Change description

The **packet-type-ignore** keyword is added.

packet-type-ignore: Ignores the protocol packet type when the device creates session entries for TCP, ICMP, or SCTP. If you do not specify this keyword, the NAT device checks the protocol packet type and creates session entries for only protocol packets that pass the check. For example, the NAT device creates session entries for TCP packets only when the packet type is SYN or ACK.

Modified feature: Static port blocks for AFT

Feature change description

As from this release, AFT supports static port blocks. AFT algorithmically creates static port block mappings based on the port block group configuration in a port block group-based IPv6-to-IPv4 source address static translation policy. A static port block mapping maps an IPv6 prefix to a unique IPv4 address and port block pair. When an IPv6-initiated session packet matches an IPv6 prefix in the policy, AFT translates the source IPv6 address of the packet into the IPv4 address and a TCP or UDP port number in the port block of the matching entry.

Command changes

New command: aft log port-block

Use **aft log port-block** to enable AFT port block logging.

Use **undo aft log port-block** to disable AFT port block logging.

Syntax

```
aft log port-block { alarm | assign | withdraw }  
undo aft log port-block { alarm | assign | withdraw }
```

Default

AFT port block logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

alarm: Enables logging for port exhaustion in an AFT port block.

assign: Enables logging for AFT port block assignment.

withdraw: Enables logging for AFT port block withdrawal.

Usage guidelines

After you configure this command, AFT generates logs when an AFT port block is assigned or withdrawn, and an AFT port block has assigned all its ports.

AFT port block logging takes effect only after you execute the **aft log enable** command to enable AFT logging.

Examples

```
# Enable AFT port block logging.  
<Sysname> system-view  
[Sysname] aft log port-block assign
```

Related commands

aft log enable

New command: aft v6tov4 source port-block-group

Use **aft v6tov4 source port-block-group** to configure a port block group-based IPv6-to-IPv4 source address static translation policy.

Use **undo aft v6tov4 source port-block-group** to delete a port block group-based IPv6-to-IPv4 source address static translation policy.

Syntax

```
aft v6tov4 source port-block-group group-id  
undo aft v6tov4 source port-block-group group-id
```

Default

No port block group-based IPv6-to-IPv4 source address static translation policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a port block group by its ID for the policy in the range of 0 to 65535.

Usage guidelines

After a policy is created, the device algorithmically maps each IPv6 prefix to a unique IPv4 address and port block pair according to the policy's port block group configuration. If not enough unique IPv4 address and port block pairs are available, excessive IPv6 prefixes will be ignored and IPv6 addresses matching those IPv6 prefixes cannot be translated.

The total number of IPv6 prefixes that can be mapped equals to the total number of unique IPv4 address and port block pairs in the policy, which is calculated as follows:

Total number of IPv6 prefixes that can be mapped = $N \times M$, where:

- N is the total number of port blocks in the port block group, which is result of dividing the port range by the port block size.
- M is the total number of IPv4 addresses in the policy available for IPv6-to-IPv4 source address translation.

For example, assuming that a policy contains two IPv4 addresses (X1 and Y1) and n port blocks. The device takes n IPv6 prefixes in the port block group, maps them to the same IPv4 address paired in turn with the first to n th port blocks. The created static port block mappings are as follows:

- IPv6 prefix $x1 \leftrightarrow$ IPv4 address X1 + Port block 1
- IPv6 prefix $x2 \leftrightarrow$ IPv4 address X1 + Port block 2
- ...
- IPv6 prefix $xn \leftrightarrow$ IPv4 address X1 + Port block n
- IPv6 prefix $y1 \leftrightarrow$ IPv4 address Y1 + Port block 1
- IPv6 prefix $y2 \leftrightarrow$ IPv4 address Y1 + Port block 2
- ...
- IPv6 prefix $yn \leftrightarrow$ IPv4 address Y1 + Port block n .

For an IPv6-initiated session packet, AFT first identifies the matching static port block mapping entry based on the IPv6 prefix that the packet's source IPv6 address matches. Then, AFT translates the source IPv6 address of the packet into the IPv4 address and a TCP or UDP port number in the port block of the matching entry.

Examples

Create AFT port block group 1. In the port block group, specify the IPv4 address range, IPv6 prefix range and prefix length, port block size, and port block range.

```
<Sysname> system-view
[Sysname] aft port-block-group 1
[Sysname-aft-port-block-group-1] address 10.1.1.1 10.1.1.15
[Sysname-aft-port-block-group-1] ipv6-prefix 100::100 100::a00 120
[Sysname-aft-port-block-group-1] block-size 1024
[Sysname-aft-port-block-group-1] port-range 1024 65535
[Sysname-aft-port-block-group-1] quit
```

Create an IPv6-to-IPv4 source address static translation policy based on port block group 1.

```
[Sysname] aft v6tov4 source port-block-group 1
```

Related commands

aft port-block-group

aft v6tov4 source

display aft configuration

New command: block-size

Use **block-size** to set the port block size for a port block group.

Use **undo block-size** to restore the default.

Syntax

block-size *block-size-value*

undo block-size

Default

The default port block size is 256.

Views

AFT port block group view

Predefined user roles

network-admin

Parameters

block-size-value: Specifies the number of ports per port block, in the range of 1 to 65535.

Usage guidelines

The port range in a port block group will be divided into port blocks of the specified port block size. AFT pairs each port block in the port range in turn with each IPv4 address and creates one-to-one mappings between the IPv4 address-port block pairs and IPv6 prefixes. Set an appropriate port block size for the port block group to meet the AFT translation requirements.

The number of ports in a port range cannot be smaller than the port block size.

Examples

```
# Set the port block size to 1024 for port block group 1.
```

```
<Sysname> system-view
```

```
[Sysname] aft port-block-group 1
```

```
[Sysname-port-block-group-1] block-size 1024
```

Related commands

aft v6tov4 source

display aft configuration

port-range

New command: ip-address

Use **ip-address** to add an IPv4 address range to an AFT port block group.

Use **undo ip-address** to remove an IPv4 address range from an AFT port block group.

Syntax

ip-address *start-address end-address* [**vpn-instance** *vpn-name*]

undo ip-address *start-address end-address* [**vpn-instance** *vpn-name*]

Default

An AFT port block group does not contain IPv4 address ranges.

Views

AFT port block group view

Predefined user roles

network-admin

Parameters

start-address end-address: Specifies the start and end IP addresses for an address range. The end address cannot be lower than the start address. If they are the same, the address range has only one IP address.

vpn-instance *vpn-name*: Specifies an MPLS L3VPN instance to which the IPv4 address or IPv4 address range belongs. The *vpn-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv4 address or IPv4 address range belongs to the public network, do not specify this option.

Usage guidelines

For IPv6-initiated session packets, a port block group-based IPv6-to-IPv4 source address translation policy translates the packets' source IPv6 addresses into IPv4 addresses in the address range of the port block group.

You can execute this command multiple times to add multiple IPv4 address ranges to a port block group. When you add address ranges to an AFT port block group, follow these guidelines:

- Each address range can contain a maximum of 256 addresses.
- The address ranges within the same port block group cannot overlap.
- Different port block groups can use overlapping address ranges but the overlapping address ranges must have non-overlapping port ranges.

Examples

```
# Add an IPv4 address range (10.1.1.1 to 10.1.1.15) to AFT port block group 1.
<Sysname> system-view
[Sysname] aft port-block-group 1
[Sysname-aft-port-block-group-1] ip-address 10.1.1.1 10.1.1.15
```

Related commands

aft v6tov4 source

display aft configuration

New command: ipv6-prefix

Use **ipv6-prefix** to add an IPv6 prefix range to an AFT port block group.

Use **undo ipv6-prefix** to remove an IPv6 prefix range from an AFT port block group.

Syntax

ipv6-prefix *ipv6-start-prefix ipv6-end-prefix prefix-length* [**vpn-instance** *vpn-name*]

undo ipv6-prefix *ipv6-start-prefix ipv6-end-prefix prefix-length* [**vpn-instance** *vpn-name*]

Default

An AFT port block group does not contain IPv6 prefix ranges.

Views

AFT port block group view

Predefined user roles

network-admin

Parameters

ipv6-start-prefix: Specifies the start IPv6 prefix of the IPv6 prefix range.

ipv6-end-prefix: Specifies the end IPv6 prefix of the IPv6 prefix range.

prefix-length: Specifies the prefix length in the range of 1 to 128.

vpn-instance *vpn-name*: Specifies an IPv6 MPLS L3VPN instance to which the IPv6 addresses belong. The *vpn-name* argument is a case-sensitive string of 1 to 31 characters. If the IPv6 addresses belong to the public network, do not specify this option.

Usage guidelines

For IPv6-initiated session packets, a port block group-based IPv6-to-IPv4 source address translation policy translates the packets' source IPv6 addresses into IPv4 addresses in the address range of the port block group.

You can execute this command multiple times to add multiple IPv6 prefix ranges to a port block group. After an IPv6-to-IPv4 source address translation policy is created based on the port block group, the device maps each IPv6 prefix to a unique IPv4 address and port block pair according to the port block group configuration. If not enough unique IPv4 address and port block pairs are available, excessive IPv6 prefixes will be ignored and IPv6 addresses matching those IPv6 prefixes cannot be translated.

The IPv6 prefix ranges within the same AFT port block group must meet the following requirements:

- IPv6 prefix ranges within the same VPN instance cannot overlap.
- IPv6 prefix ranges that belong to the public network cannot overlap.

The IPv6 prefix ranges in different AFT port block groups must meet the following requirements:

- IPv6 prefix ranges in the same VPN instance cannot overlap.
- IPv6 prefix ranges that belong to the public network can overlap.

Examples

```
# Add an IPv6 prefix range (240E:00D8:8200:0000::/64 to 240E:00D8:8200:0007::/64) to AFT port
block group 1.
<Sysname> system-view
[Sysname] aft port-block-group 1
[Sysname-aft-port-block-group-1] ipv6-prefix 240E:00D8:8200:0000:: 240E:00D8:8200:0007::
64
```

Related commands

aft v6tov4 source

display aft configuration

New command: port-range

Use **port-range** to specify the port range for an AFT port block group.

Use **undo port-range** to restore the default port range for an AFT port block group.

Syntax

port-range *start-port-number end-port-number*

undo port-range

Default

An AFT port block group uses port range 1 to 65535.

Views

AFT port block group view

Predefined user roles

network-admin

Parameters

start-port-number end-port-number: Specifies the start and end port numbers for the port range. The end port number cannot be lower than the start port number. As a best practice, set the start port number to 1024 or higher to avoid application protocol identification errors.

Usage guidelines

The port range in a port block group will be divided into port blocks of the specified port block size.

The number of ports in a port range cannot be smaller than the port block size.

Examples

Specify port range 1024 to 65535 for AFT port block group 1.

```
<Sysname> system-view
```

```
[Sysname] aft port-block-group 1
```

```
[Sysname-aft-port-block-group-1] port-range 1024 65535
```

Related commands

aft port-block-group

aft v6tov4 source

block-size

display aft configuration

Modified command: display aft configuration

Syntax

display aft configuration

Views

Any view

Change description

The **aft port-block-group XX** field is added to the command output.

aft port-block-group XX: AFT port block identified by ID XX. An AFT port block group contains the following settings:

- **ip-address**—IPv4 address ranges used for IPv6-to-IPv4 source address translation.
- **ipv6-prefix**—IPv6 prefix ranges for IPv6-to-IPv4 source address translation.
- **block-size**—Port block size of the port block group.
- **port-range**—Port range of the port block group.

Modified command: display aft port-block

Old syntax

In standalone mode:

display aft port-block

In IRF mode:

display aft port-block [**slot** *slot-number*]

New syntax

In standalone mode:

display aft port-block { **dynamic** | **static** }

In IRF mode:

display aft port-block { **dynamic** | **static** } [**slot** *slot-number*]

Views

Any view

Change description

The **dynamic** and **static** keywords are added to the command syntax and the **IPv6 Prefix** field is added to the command output.

dynamic: Specifies dynamic port block mappings.

static: Specifies static port block mappings.

IPv6 Prefix: IPv6 prefix to match the IPv6 addresses to be translated. This field is available only in static port block mappings.

New feature: Support of URL-based automatic configuration for encryption

The URL for URL-based automatic configuration can be in either of the following forms:

- **Plaintext form**—The user directly configures the plaintext URL. Parameters in the URL are configured and transmitted in plaintext form.
- **Encrypted form**—The administrator generates the encrypted URL and an authentication password for the URL by using the controller. Within the validity of the URL, a user can enter the authentication password as prompted to use the URL to perform URL-based automatic configuration.

New feature: Support of USB-based automatic configuration for encryption

The configuration file for USB-based automatic configuration can be in either of the following forms:

- **Plaintext form**—The configuration file is saved in plaintext form.
- **Encrypted form**—The configuration file is generated by the administrator in encrypted form by using the controller. When being transmitted to a USB disk, the configuration data in the file is transmitted in encrypted form. When being used to perform automatic configuration, the configuration data is automatically decrypted by the device.

New feature: Configuring DNS redirection

Configuring DNS redirection

About this task

DNS redirection applies to the scenarios that require DNS request distribution.

With DNS redirection enabled, the device monitors the received DNS requests (only UDP packets are supported in the current software version) and resolves the source IP addresses, source port numbers, and domain names. Then, the device searches for a matching domain name rule and redirects the request to the DNS server in the rule.

The device enabled with DNS redirection works as follows:

1. The device searches for a matching domain name rule.
 - If a match is found, it replaces the destination IP address in the request with the IP address of the first reachable DNS server in the server group bound to the rule. Then, the device forwards the request to the DNS server.
 - If no match is found, the device does not redirect the DNS request.
2. The device records the replacement, including the source IP address, source port number, and requested server address in the DNS request, and the replaced server address.
3. Upon receiving the DNS reply, the device replaces the source IP address in the reply with the original server address in the request.

Restrictions and guidelines

The DNS redirection and DNS transparent proxy features cannot be both configured.

Procedure

1. Enter system view.
system-view
2. Enable DNS redirection.
dns redirect enable
By default, DNS redirection is disabled.

Command reference

New command: dns redirect enable

Use **dns redirect enable** to enable DNS redirection.

Use **undo dns redirect enable** to disable DNS redirection.

Syntax

dns redirect enable

undo dns redirect enable

Default

DNS redirection is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With DNS redirection enabled, the device monitors the received DNS requests (only UDP packets are supported in the current software version) and resolves the source IP addresses, source port numbers, and domain names. Then, the device searches for a matching domain name rule and redirects the request to the DNS server in the rule.

The device enabled with DNS redirection works as follows:

1. The device searches for a matching domain name rule.
 - If a match is found, it replaces the destination IP address in the request with the IP address of the first reachable DNS server in the server group bound to the rule. Then, the device forwards the request to the DNS server.
 - If no match is found, the device does not redirect the DNS request.
2. The device records the replacement, including the source IP address, source port number, and requested server address in the DNS request, and the replaced server address.
3. Upon receiving the DNS reply, the device replaces the source IP address in the reply with the original server address in the request.

This configuration applies to both IPv4 DNS redirection and IPv6 DNS redirection.

The **dns redirect enable** and **dns transparent-proxy enable** commands are mutually exclusive. After one command is executed, the other command cannot be executed.

Examples

```
# Enable DNS redirection.  
<Sysname> system-view  
[Sysname] dns redirect enable
```

New feature: Enabling DNS server health check

Enabling DNS server health check

About this task

This feature enables the device to detect the availability of DNS servers in a DNS server group, which prevents the device from forwarding packets to unavailable DNS servers.

When the device enabled with DNS redirection receives a DNS request that matches a domain name rule, the device forwards the request to a DNS server. The DNS server is selected according to the server order displayed in the **display this** command.

If the device does not receive a DNS reply from the DNS server within two seconds, it reselects a DNS server. To prevent the device from selecting an unavailable DNS server, execute the **health-check enable** command to detect the availability of DNS servers. After you execute the command on the device, it works as follows:

1. The device periodically sends a DNS request to each DNS server in the DNS server group.
2. If the device receives a DNS reply from a DNS server, it regards the DNS server available.
3. If the device does not receive any DNS reply from a DNS server after it sends a DNS request to the DNS server for three consecutive times, it regards the DNS server unavailable.

4. Upon receiving a DNS request that matches a domain name rule, the device ignores the unavailable DNS servers automatically and selects a DNS server according to the lexicographical order.

Restrictions and guidelines

In a scenario disabled with DNS redirection, as a best practice to prevent the device from periodically sending DNS requests, disable DNS server health check.

Procedure

1. Enter system view.
system-view
2. Create a DNS server group and enter its view.
dns server-group *group-id* [**vpn-instance** *vpn-instance-name*]
3. Enable DNS server health check.
health-check enable
By default, DNS server health check is disabled.

Command reference

New command: health-check enable

Use **health-check enable** to enable DNS server health check.

Use **undo health-check enable** to disable DNS server health check.

Syntax

health-check enable
undo health-check enable

Default

DNS server health check is disabled.

Views

DNS server group view

Predefined user roles

network-admin

Usage guidelines

When the device enabled with DNS redirection receives a DNS request that matches a domain name rule, the device forwards the request to a DNS server. The DNS server is selected according to the server order displayed in the **display this** command.

If the device does not receive a DNS reply from the DNS server within two seconds, it reselects a DNS server. To prevent the device from selecting an unavailable DNS server, execute the **health-check enable** command to detect the availability of DNS servers. After you execute the command on the device, it works as follows:

1. The device periodically sends a DNS request to each DNS server in the DNS server group.
2. If the device receives a DNS reply from a DNS server, it regards the DNS server available.

3. If the device does not receive any DNS reply from a DNS server after it sends a DNS request to the DNS server for three consecutive times, it regards the DNS server unavailable.
4. Upon receiving a DNS request that matches a domain name rule, the device ignores the unavailable DNS servers automatically and selects a DNS server according to the lexicographical order.

Examples

Enable health check for DNS servers in DNS server group 1.

```
<Sysname> system-view  
[Sysname] dns server-group 1  
[Sysname-server-group-1] health-check enable
```

Related commands

display dns server health status

New feature: Disabling receiving a specific type of ICMPv6 messages

Disabling receiving a specific type of ICMPv6 messages

About this task

By default, the device receives all types of ICMPv6 messages. Such a setting might affect device performance if a large number of ICMPv6 responses are received within a short time. To resolve this issue, you can perform this task to disable the device from receiving a specific type of ICMPv6 messages.

Restrictions and guidelines

Disabling receiving ICMPv6 messages of a specific type might affect network operation. Please use this feature with caution.

Procedure

1. Enter system view.
system-view
2. Disable the device from receiving a specific type of ICMPv6 messages.
undo ipv6 icmpv6 { name *name* | type *type* code *code* } receive enable
By default, the device receives ICMPv6 messages of all types.

Command reference

ipv6 icmpv6 receive enable

Use **ipv6 icmpv6 receive enable** to enable the device to receive a specific type of ICMPv6 messages.

Use **undo ipv6 icmpv6 receive enable** to disable the device from receiving a specific type of ICMPv6 messages.

Syntax

```
ipv6 icmpv6 { name name | type type code code } receive enable  
undo ipv6 icmpv6 { name name | type type code code } receive enable
```

Default

The device receives all types of ICMPv6 messages.

Views

System view

Predefined user roles

network-admin

Parameters

name *name*: Specifies an ICMPv6 message name.

type *type*: Specifies an ICMPv6 message type. The value range for the *type* argument is 0 to 255.

code *code*: Specifies an ICMPv6 message code. The value range for the *code* argument is 0 to 255.

Usage guidelines



CAUTION:

Disabling receiving ICMPv6 messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device receives all types of ICMPv6 messages. Such a setting might affect device performance if a large number of ICMPv6 responses are received within a short time. To resolve this issue, you can use this command to disable the device from receiving a specific type of ICMPv6 messages.

Table 75 shows common ICMPv6 messages and their meanings.

Table 75 Common ICMPv6 messages

Name	Type	Code	Description
echo	128	0	Echo request used to ping a target node.
echo-reply	129	0	Echo reply sent by a target node after receiving an echo request.
err-header-field	4	0	Erroneous header field was found.
frag-time-exceeded	3	1	Fragment reassembly timed out.
hop-limit-exceeded	3	0	Hop limit decreased to 0 in transit.
host-admin-prohib	1	1	Communication with the target host was prohibited by the admin policy.
host-unreachable	1	3	The target host address was unreachable.
neighbor-advertisement	136	0	Neighbor advertisement for IPv6 neighbor discovery.
neighbor-solicitation	135	0	Neighbor solicitation for IPv6 neighbor discovery.
network-unreachable	1	0	No route to destination exists.
packet-too-big	2	0	Packet forwarding failed because the packet length was longer than the MTU.
port-unreachable	1	4	The target port was unreachable.

Name	Type	Code	Description
redirect	137	0	Route redirection message.
router-advertisement	134	0	IPv6 router advertisement.
router-solicitation	133	0	IPv6 router solicitation.
unknown-ipv6-opt	4	2	Unknown IPv6 option.
unknown-next-hdr	4	1	Unknown IPv6 Next Header field.

Examples

Disable the device from receiving ICMPv6 echo reply messages.

```
<Sysname> system-view
```

```
[Sysname] undo ipv6 icmpv6 name echo-reply receive enable
```

New feature: Disabling sending a specific type of ICMPv6 messages

Disabling sending a specific type of ICMPv6 messages

About this task

By default, the device sends all types of ICMPv6 messages except Destination Unreachable and Redirect messages. Attackers might obtain device information from specific types of ICMPv6 messages, causing security issues.

For security purposes, you can perform this task to disable the device from sending specific types of ICMPv6 messages.

Restrictions and guidelines

Disabling sending ICMPv6 messages of a specific type might affect network operation. Please use this feature with caution.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following tasks:

- Execute the **ipv6 icmpv6 send enable** command.
- Execute one of the following commands as needed:
 - **ipv6 unreachable enable**
 - **ipv6 hoplimit-expires enable**
 - **ipv6 redirects enable**

Procedure

1. Enter system view.
system-view
2. Disable the device from sending a specific type of ICMPv6 messages.
undo ipv6 icmpv6 { name *name* | type *type* code *code* } send enable

By default, the device can send all types of ICMPv6 messages except Destination Unreachable and Redirect messages.

Command reference

ipv6 icmpv6 send enable

Use **ipv6 icmpv6 send enable** to enable the device to send a specific type of ICMPv6 messages.

Use **undo ipv6 icmpv6 send enable** to disable the device from sending a specific type of ICMPv6 messages.

Syntax

```
ipv6 icmpv6 { name name | type type code code } send enable
undo ipv6 icmpv6 { name name | type type code code } send enable
```

Default

The device can send all types of ICMPv6 messages except Destination Unreachable and Redirect messages.

Views

System view

Predefined user roles

network-admin

Parameters

- name** *name*: Specifies an ICMPv6 message name.
- type** *type*: Specifies an ICMPv6 message type. The value range for the *type* argument is 0 to 255.
- code** *code*: Specifies an ICMPv6 message code. The value range for the *code* argument is 0 to 255.

Usage guidelines



CAUTION:

Disabling sending ICMPv6 messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device sends all types of ICMPv6 messages except Destination Unreachable and Redirect messages. Attackers might obtain device information from specific types of ICMPv6 messages, causing security issues.

For security purposes, you can use this command to disable the device from sending specific types of ICMPv6 messages.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following tasks:

- Execute the **ipv6 icmpv6 send enable** command.
- Execute one of the following commands as needed:
 - **ipv6 unreachable enable**
 - **ipv6 hoplimit-expires enable**
 - **ipv6 redirects enable**

Table 76 shows common ICMPv6 messages and their meanings.

Table 76 Common ICMPv6 messages

Name	Type	Code	Description
echo	128	0	Echo request used to ping a target node.
echo-reply	129	0	Echo reply sent by a target node after receiving an echo request.
err-header-field	4	0	Erroneous header field was found.
frag-time-exceeded	3	1	Fragment reassembly timed out.
hop-limit-exceeded	3	0	Hop limit decreased to 0 in transit.
host-admin-prohib	1	1	Communication with the target host was prohibited by the admin policy.
host-unreachable	1	3	The target host address was unreachable.
neighbor-advertisement	136	0	Neighbor advertisement for IPv6 neighbor discovery.
neighbor-solicitation	135	0	Neighbor solicitation for IPv6 neighbor discovery.
network-unreachable	1	0	No route to destination exists.
packet-too-big	2	0	Packet forwarding failed because the packet length was longer than the MTU.
port-unreachable	1	4	The target port was unreachable.
redirect	137	0	Route redirection message.
router-advertisement	134	0	IPv6 router advertisement.
router-solicitation	133	0	IPv6 router solicitation.
unknown-ipv6-opt	4	2	Unknown IPv6 option.
unknown-next-hdr	4	1	Unknown IPv6 Next Header field.

Examples

```
# Disable the device from sending ICMPv6 echo reply messages.
```

```
<Sysname> system-view
```

```
[Sysname] undo ipv6 icmpv6 name echo-reply send enable
```

Related commands

ipv6 hoplimit-expires enable

ipv6 redirects enable

ipv6 unreachable enable

New feature: Enabling advertising invalid delegated prefixes

Enabling advertising invalid delegated prefixes

About this task

An interface can generate an IPv6 address based on a prefix, which is assigned by the DHCPv6 server. When the assigned prefix goes invalid, the device does not advertise RA messages for the

event by default. In this case, endpoints that use this prefix are not aware of the event, and continue using the IPv6 addresses generated based on the prefix, causing communication failures. To avoid this problem, you can use this feature.

When a DHCPv6 server-assigned prefix goes invalid, the device sends out RA messages immediately. The device sets both the preferred lifetime and valid lifetime to 0 in these messages, announcing that the prefix is invalid. Upon receiving the advertisement, endpoints will no longer use the IPv6 addresses generated based on the prefix. For more information about DHCPv6, see DHCPv6 configuration in *Layer 3—IP Services Configuration Guide*.

Restrictions and guidelines

RA message advertisement is suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Enable advertising invalid delegated prefixes.
ipv6 nd ra invalid-delegated-prefix advertise enable
By default, advertising invalid delegated prefixes is disabled.

Command reference

ipv6 nd ra invalid-delegated-prefix advertise enable

Use **ipv6 nd ra invalid-delegated-prefix advertise enable** to enable advertising invalid delegated prefixes.

Use **undo ipv6 nd ra invalid-delegated-prefix advertise enable** to disable advertising invalid delegated prefixes.

Syntax

ipv6 nd ra invalid-delegated-prefix advertise enable
undo ipv6 nd ra invalid-delegated-prefix advertise enable

Default

Advertising invalid delegated prefixes is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

An interface can generate an IPv6 address based on a prefix, which is assigned by the DHCPv6 server. When the assigned prefix goes invalid, the device does not advertise RA messages for the event by default. In this case, endpoints that use this prefix are not aware of the event, and continue using the IPv6 addresses generated based on the prefix, causing communication failures. To avoid this problem, you can use this feature.

When a DHCPv6 server-assigned prefix goes invalid, the device sends out RA messages immediately. The device sets both the preferred lifetime and valid lifetime to 0 in these messages, announcing that the prefix is invalid. Upon receiving the advertisement, endpoints will no longer use the IPv6 addresses generated based on the prefix. For more information about DHCPv6, see DHCPv6 configuration in *Layer 3—IP Services Configuration Guide*.

RA message advertisement is suppressed by default. To disable RA message suppression, use the **undo ipv6 nd ra halt** command.

Examples

```
# Enable advertising invalid delegated prefixes on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra invalid-delegated-prefix advertise enable
```

Related commands

ipv6 dhcp client pd

ipv6 nd ra halt

New feature: Setting the TTL value for DNS entries

Setting the TTL value for DNS entries

About this task

The device periodically sends a DNS request to the DNS server according to the TTL for DNS entries, which consumes CPU resources. If the TTL value is too small, the device sends DNS requests frequently to the DNS server, which consumes more CPU resources. If the TTL value is too large, DNS mappings cannot be updated in time. To avoid such issues, you can use this command to set the TTL value for DNS entries.

By default, the DNS client obtains the TTL for DNS entries in the dynamic domain name resolution cache from the DNS reply:

After you set the TTL value for DNS entries, the device specifies the TTL for DNS entries as follows:

- If the TTL value in the DNS reply is smaller than the minimum TTL value, the device uses the minimum TTL value as the TTL for DNS entries. If the TTL value is greater than or equal to the minimum TTL value, the device uses the TTL value in the DNS reply as the TTL for DNS entries.
- If the TTL value in the DNS reply is greater than the maximum TTL value, the device uses the maximum TTL value as the TTL for DNS entries. If the TTL value is smaller than or equal to the maximum TTL value, the device uses the TTL value in the DNS reply as the TTL for DNS entries.

Restrictions and guidelines

After you configure the TTL value for DNS entries, the configuration takes effect only on the subsequent DNS entries.

After you execute the **undo dns cache ttl** command, the current TTL for the existing DNS entries still works.

If you do not specify any keywords when you execute the **undo dns cache ttl** command, this command cancels all TTL configuration for DNS entries.

The value for the minimum TTL value must be smaller than that for the maximum TTL value.

If you execute the **dns cache ttl minimum**, **dns cache ttl maximum**, or **dns cache ttl minimum maximum** command multiple times, the most recent configuration takes effect.

Procedure

1. Enter system view.
system-view
2. (Optional.) Set the TTL value for DNS entries.
dns cache ttl { maximum *max-value* | minimum *min-value* } *
By default, the TTL value for DNS entries is the TTL value in the DNS reply.

Command reference

New command: dns cache ttl

Use **dns cache ttl** to set the TTL value for DNS entries.

Use **undo dns cache ttl** to cancel the TTL configuration for DNS entries.

Syntax

```
dns cache ttl { maximum max-value | minimum min-value } *  
undo dns cache ttl [ maximum | minimum ]
```

Default

The TTL value for DNS entries is the TTL value in the DNS reply.

Views

System view

Predefined user roles

network-admin

Parameters

maximum *max-value*: Specifies the maximum TTL value for DNS entries, in the range of 60 to 3600 seconds.

minimum *min-value*: Specifies the minimum TTL value for DNS entries, in the range of 60 to 3600 seconds. The value for the *min-value* argument must be smaller than that for the *max-value* argument.

Usage guidelines

Application scenarios

The device periodically sends a DNS request to the DNS server according to the TTL for DNS entries, which consumes CPU resources. If the TTL value is too small, the device sends DNS requests frequently to the DNS server, which consumes more CPU resources. If the TTL value is too large, DNS mappings cannot be updated in time. To avoid such issues, you can use this command to set the TTL value for DNS entries.

Operating mechanism

By default, the DNS client obtains the TTL for the following DNS entries from the DNS reply:

- DNS entries generated from DNS transparent proxy.
- DNS entries generated from DNS snooping.

- Dynamic domain name resolution cache generated from the DNS server/DNS server group.
After you set the TTL value for DNS entries, the device specifies the TTL for DNS entries as follows:
- If the TTL value in the DNS reply is smaller than the minimum TTL value, the device uses the minimum TTL value as the TTL for DNS entries. If the TTL value is greater than or equal to the minimum TTL value, the device uses the TTL value in the DNS reply as the TTL for DNS entries.
- If the TTL value in the DNS reply is greater than the maximum TTL value, the device uses the maximum TTL value as the TTL for DNS entries. If the TTL value is smaller than or equal to the maximum TTL value, the device uses the TTL value in the DNS reply as the TTL for DNS entries.

Restrictions and guidelines

After you execute this command, the configuration only takes effect on the subsequent DNS entries generated from DNS transparent proxy, DNS snooping, and DNS server/DNS server group.

After you execute the **undo dns cache ttl** command, the current TTL for the existing DNS entries still works.

If you do not specify any keywords when you execute the **undo dns cache ttl** command, this command cancels all TTL configuration for DNS entries.

If you execute the **dns cache ttl minimum**, **dns cache ttl maximum**, or **dns cache ttl minimum maximum** command multiple times, the most recent configuration takes effect.

Examples

Set the maximum TTL value for DNS entries to 3600 seconds and the minimum TTL value for DNS entries to 180 seconds.

```
<Sysname> system-view
[Sysname] dns cache ttl maximum 3600 minimum 180
```

Related commands

dns server
dns server-group
dns snooping enable
dns transparent-proxy enable

New feature: Configuring DNS filtering

Configuring DNS filtering

About this task

Enabled with DNS filtering, the DNS proxy matches the domain names in DNS requests with the host names on the allowlist or denylist to filter DNS requests.

The DNS proxy uses DNS filtering to filter DNS requests as follows:

- If the allowlist has a matching host name or the denylist has no matching host name with the domain name in the received DNS request, the DNS proxy forwards the request. After receiving a DNS reply, the DNS proxy records the DNS mapping and forwards the reply to the DNS client.
- If the denylist has a matching host name or the allowlist has no matching host name with the domain name in the received DNS request, the DNS proxy discards the DNS request.

To implement a strict access control, use an allowlist to filter DNS requests. To implement a loose access control, use a denylist to filter DNS requests.

Restrictions and guidelines

You can add multiple host names to an allowlist or denylist. Do not add a host name to both a denylist and an allowlist.

Procedure

1. Enter system view.
system-view
2. Enable DNS filtering and add a host name to the allowlist or denylist.
dns filter { allowlist | denylist } hostname
By default, DNS filtering is disabled.

Command reference

New command: dns filter

Use **dns filter** to enable DNS filtering and add a host name to the denylist or allowlist.

Use **undo dns filter** to disable DNS filtering and delete a host name from the denylist or allowlist.

Syntax

dns filter { allowlist | denylist } hostname
undo dns filter { allowlist | denylist } hostname

Default

DNS filtering is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

allowlist: Adds a host name to the allowlist.

denylist: Adds a host name to the denylist.

hostname: Specifies a host name, a case-insensitive string of 1 to 253 characters. The string can contain letters, digits, hyphens (-), underscores (_), and dots (.). This argument supports fuzzy match by adding a wildcard (*) to the host name. For example, to match a host name including **abc**, specify the **hostname** argument as ***abc***, ***abc**, or **abc***. To exactly match a host name, do not add the wildcard (*).

Usage guidelines

The DNS proxy uses DNS filtering to filter DNS requests as follows:

- If the allowlist has a matching host name or the denylist does not have any matching host name with the domain name in the received DNS request, the DNS proxy forwards the request. Upon receiving a DNS reply, the DNS proxy records the DNS mapping and forwards the reply to the DNS client.
- If the denylist has a matching host name or the allowlist does not have any matching host name with the domain name in the received DNS request, the DNS proxy discards the DNS request.

To implement a strict access control, use an allowlist to filter DNS requests. To implement a loose access control, use a denylist to filter DNS requests.

To add multiple host names to the allowlist or denylist, repeat this command. However, a host name cannot be added to both the denylist and allowlist.

Examples

```
# Enable DNS filtering and add the host names containing .abc to the allowlist.
```

```
<Sysname> system-view
```

```
[Sysname] dns filter allowlist *.abc
```

New feature: Configuring DNS snooping

Configuring DNS snooping

About this task

DNS snooping is applicable to scenarios that use domain name-based policies (such as security policies and bandwidth policies). In such a scenario, the device requires the resolved IP addresses for traffic filtering. Enabled with DNS snooping, the device monitors received DNS requests and replies, and works as follows:

- If the domain name in a DNS request matches a policy, the device records the DNS mapping after receiving the DNS reply, and reports the mapping to the policy for traffic filtering.
- If the domain name does not match a policy, the device does not record the DNS mapping.

Restrictions and guidelines

DNS snooping is applicable to only Layer 3 service networks. Layer 2 forwarding services belonging to the same VLAN on the device do not support DNS snooping.

DNS snooping works only between the DNS client and DNS server, or the DNS client and DNS proxy.

The DNS snooping and DNS transparent proxy features cannot be both configured.

The DNS snooping feature cannot be used across VPNs. Make sure the input and output interfaces of DNS packets on the device belong to the same VPN.

Procedure

1. Enter system view.

system-view

2. (Optional.) Set the TTL value for DNS entries.

dns cache ttl { maximum *max-value* | minimum *min-value* } *

By default, the TTL value for DNS entries is the TTL value in the DNS reply.

3. Enable DNS snooping.

dns snooping enable

By default, DNS snooping is disabled.

Command reference

New command: dns snooping enable

Use **dns snooping enable** to enable DNS snooping.

Use **undo dns snooping enable** to disable DNS snooping.

Syntax

dns snooping enable
undo dns snooping enable

Default

DNS snooping is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DNS snooping is applicable to scenarios that use domain name-based policies (such as security policies and bandwidth policies). In such a scenario, the device requires the resolved IP addresses for traffic filtering. Enabled with DNS snooping, the device monitors received DNS requests and replies, and works as follows:

- If the domain name in a DNS request matches a policy, the device records the DNS mapping after receiving the DNS reply, and reports the mapping to the policy for traffic filtering.
- If the domain name does not match a policy, the device does not record the DNS mapping.

DNS snooping is applicable to only Layer 3 service networks. Layer 2 forwarding services belonging to the same VLAN on the device do not support DNS snooping.

DNS snooping works only between the DNS client and DNS server, or the DNS client and DNS proxy.

The DNS snooping and DNS transparent proxy features cannot be both configured.

The DNS snooping feature cannot be used across VPNs. Make sure the input and output interfaces of DNS packets on the device belong to the same VPN.

Examples

```
# Enable DNS snooping.  
<Sysname> system-view  
[Sysname] dns snooping enable
```

Related commands

dns transparent-proxy enable

New feature: Configuring the DNS transparent proxy

Configuring the DNS transparent proxy

About this task

DNS transparent proxy modifies the source address in DNS requests so that the DNS client seems to receive a DNS reply directly from the DNS server. This feature is applicable to domain name-based policies, such as security policies and bandwidth policies.

The DNS client does not configure the DNS server address as the DNS transparent proxy address, which simplifies the DNS client configuration. As a best practice, enable DNS transparent proxy in some load balancing scenarios.

The device enabled with DNS transparent proxy monitors received DNS requests and replies and records DNS mappings as follows:

1. The device monitors all received DNS packets. Upon receiving a DNS request, the device specifies a local IP address that can reach the DNS server as the source IP address for the request.
2. Upon receiving the DNS reply, the device records the DNS mapping and forwards the reply to the DNS client.
3. The device searches the local entries after receiving another request. If a match is found, the device returns a DNS reply to the client. If no match is found, the device forwards the query to the DNS server for domain name resolution.

Restrictions and guidelines

Do not configure the DNS transparent proxy feature together with the following features:

- DNS fast-reply.
- DNS snooping.
- DNS redirection.

The DNS transparent proxy feature cannot be used across VPNs. Make sure the input and output interfaces of DNS packets on the device belong to the same VPN.

Procedure

1. Enter system view.
system-view
2. (Optional.) Set the TTL value for DNS entries.
dns cache ttl { maximum *max-value* | minimum *min-value* } *
By default, the TTL value for DNS entries is the TTL value in the DNS reply.
3. Enable DNS transparent proxy.
dns transparent-proxy enable
By default, DNS transparent proxy is disabled.

Command reference

New command: dns transparent-proxy enable

Use **dns transparent-proxy enable** to enable DNS transparent proxy.

Use **undo dns transparent-proxy enable** to disable DNS transparent proxy.

Syntax

dns transparent-proxy enable
undo dns transparent-proxy enable

Default

DNS transparent proxy is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DNS transparent proxy modifies the source address in DNS requests so that the DNS client seems to receive a DNS reply directly from the DNS server. This feature is applicable to domain name-based policies, such as security policies and bandwidth policies.

The DNS client does not configure the DNS server address as the DNS transparent proxy address, which simplifies the DNS client configuration. As a best practice, enable DNS transparent proxy in some load balancing scenarios.

The device enabled with DNS transparent proxy monitors received DNS requests and replies and records DNS mappings as follows:

1. The device monitors all received DNS packets. Upon receiving a DNS request, the device specifies a local IP address that can reach the DNS server as the source IP address for the request.
2. Upon receiving the DNS reply, the device records the DNS mapping and forwards the reply to the DNS client.
3. The device searches the local entries after receiving another request. If a match is found, the device returns a DNS reply to the client. If no match is found, the device forwards the query to the DNS server for domain name resolution.

Do not configure the DNS transparent proxy feature together with the following features:

- DNS fast-reply.
- DNS snooping.
- DNS redirection.

The DNS transparent proxy feature cannot be used across VPNs. Make sure the input and output interfaces of DNS packets on the device belong to the same VPN.

Examples

```
# Enable DNS transparent proxy.  
<Sysname> system-view  
[Sysname] dns transparent-proxy enable
```

Related commands

dns fast-reply enable

dns proxy enable

dns redirect enable

dns snooping enable

Modified feature: Displaying the running configuration

Feature change description

As from this release, the device can display the running configuration by section.

Command changes

Modified command: display current-configuration

Old syntax

```
display current-configuration [ configuration [ module-name ] ] | controller |  
exclude-provision | interface [ interface-type [ interface-number ] ] | vpn-instance  
[ vpn-instance-name ] | vsys vsys-name ]
```

New syntax

```
display current-configuration [ configuration [ module-name ] ] | controller |  
exclude-provision | interface [ interface-type [ interface-number ] ] | vpn-instance  
[ vpn-instance-name ] | vsys vsys-name ] [ by-section { begin | exclude | include }  
regular-expression ]
```

View

Any view

Change description

Before modification: The command does not support the **by-section** { **begin** | **exclude** | **include** } option.

After modification: The command supports the **by-section** { **begin** | **exclude** | **include** } option.

by-section: Displays the running configuration by section. Each section contains the configuration in a command view and two adjacent sections are separated by a pound sign (#). If you do not specify this keyword, the command displays the running configuration by line.

begin: Displays the first configuration section that matches the specified regular expression and all subsequent configuration sections.

exclude: Displays all configuration sections not matching the specified regular expression.

include: Displays all configuration sections matching the specified regular expression.

regular-expression: Specifies a regular expression to filter the configuration sections, a case-sensitive string of 1 to 256 characters. A section matches the specified regular expression if it contains command lines that match the specified regular expression.

Modified feature: Displaying the contents of the configuration file for the next system startup

Feature change description

As from this release, the device can display the contents of the configuration file for the next system startup by section.

Command changes

Modified command: display saved-configuration

Old syntax

display saved-configuration

New syntax

display saved-configuration [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Change description

Before modification: The command does not support the **by-section** { **begin** | **exclude** | **include** } option.

After modification: The command supports the **by-section** { **begin** | **exclude** | **include** } option.

by-section: Displays the configuration used at the next startup by section. Each section contains the configuration in a command view and two adjacent sections are separated by a pound sign (#). If you do not specify this keyword, the command displays the configuration used at the next startup by line.

begin: Displays the first configuration section that matches the specified regular expression and all subsequent configuration sections.

exclude: Displays all configuration sections not matching the specified regular expression.

include: Displays all configuration sections matching the specified regular expression.

regular-expression: Specifies a regular expression to filter the configuration sections, a case-sensitive string of 1 to 256 characters. A section matches the specified regular expression if it contains command lines that match the specified regular expression.

Modified feature: Displaying the running configuration in the current view

Feature change description

As from this release, the device can display the running configuration in the current view by section.

Command changes

Modified command: display this

Old syntax

display this

New syntax

display this [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Change description

Before modification: The command does not support the **by-section** { **begin** | **exclude** | **include** } option.

After modification: The command supports the **by-section** { **begin** | **exclude** | **include** } option.

by-section: Displays the running configuration in the current view by section. Each section contains the configuration in a command view and two adjacent sections are separated by a pound sign (#). If you do not specify this keyword, the command displays the running configuration in the current view by line.

begin: Displays the first configuration section that matches the specified regular expression and all subsequent configuration sections.

exclude: Displays all configuration sections not matching the specified regular expression.

include: Displays all configuration sections matching the specified regular expression.

regular-expression: Specifies a regular expression to filter the configuration sections, a case-sensitive string of 1 to 256 characters. A section matches the specified regular expression if it contains command lines that match the specified regular expression.

Modified feature: Configuring an ACL match criterion

Feature change description

As from this release, you can specify the **raw-vpn** keyword in the **if-match acl** command.

Command changes

Modified: if-match

Old syntax

```
if-match acl [ ipv6 | mac ] { acl-number | name acl-name } [ mpls-inner ]
```

New syntax

```
if-match acl [ ipv6 | mac ] { acl-number | name acl-name } [ mpls-inner | raw-vpn ]
```

Views

Traffic class view

Change description

The **raw-vpn** keyword is added.

raw-vpn: Enables the ACL to match a packet after NAT is performed on the packet. If you do not specify this keyword, the device performs ACL matching before performing NAT. In this case, the source IP addresses of different private network users might be translated to the same public IP address, and the traffic class cannot identify return packets of different private network users. This keyword can only be used on a public network interface that is configured with the **nat outbound** command and uses an ACL to match return packets.

Modified feature: Adding a node to a SID list

Feature change description

Before you specify a SID list for a candidate path in an SRv6 TE policy, you need to create the SID list and add nodes to the SID list. After you add nodes to a SID list, the system will sort the nodes in ascending order of node index. The node with the smallest index represents the next hop of the source node on the forwarding path.

As from this version, the device supports using four 32-bit G-SIDs to represent one normal 128-bit SRv6 SID to reduce the SRH cost. In a SID list, you can add a 128-bit SRv6 SID with a COC flavor, indicating that the next node of the current node is a 32-bit G-SID. For more information about G-SIDs, see IPv6 Segment Routing configuration.

Command changes

Modified command: index

Use **index** to add a node to a SID list.

Use **undo index** to delete a node from a SID list.

Old syntax

index *index-number* **ipv6** *ipv6-address*

undo index *index-number*

New syntax

index *index-number* **ipv6** *ipv6-address*

index *index-number* **coc32** **ipv6** *ipv6-address* *common-prefix-length*

undo index *index-number*

Views

SID list view

Change description

The following parameters were added:

- **coc32**: Adds the COC flavor. It indicates that the next node of the current node is a 32-bit G-SID.
- *common-prefix-length*: Specifies the length of the common prefix of the next G-SID. The value range for this argument is 1 to 94.

Modified feature: Configuring a traffic redirection action

Feature change description

As from this release, you can configure an action of redirecting traffic to an SRv6 TE policy.

Command changes

Modified: redirect

Old syntax

```
redirect interface interface-type interface-number [ track-oap ]  
undo redirect interface interface-type interface-number
```

New syntax

```
redirect interface interface-type interface-number [ track-oap ]  
undo redirect interface interface-type interface-number  
redirect srv6-policy endpoint color [ { sid | vpnsid } sid ]  
undo redirect srv6-policy
```

Views

Traffic behavior view

Change description

The following parameter is added:

srv6-policy *endpoint color* [{ **sid** | **vpnsid** } *sid*] : Redirects traffic to an SRv6 TE policy. The *endpoint* argument represents the endpoint IPv6 address of the SRv6 TE policy. The *color* argument represents the color attribute value of the SRv6 TE policy, in the range of 0 to 4294967295. The **sid** *sid* argument represents the SRv6 SID (an IPv6 address) of the egress node. Packets continue to be forwarded in the public network after they are forwarded through the SRv6 TE policy. The **vpnsid** *sid* argument represents the SRv6 SID (an IPv6 address) of the egress node. Packets continue to be forwarded in the private network after they are forwarded through the SRv6 TE policy. The device adds the SRv6 SID to the SRH header and places it after the SID list. After the packets are forwarded to the egress node, the egress node takes the forwarding action based on the SRv6 SID.

Modified feature: Clearing forwarding statistics for all SRv6 TE policies

Feature change description

As from this release, you can configure an action of redirecting traffic to an SRv6 TE policy.

Command changes

Modified: reset segment-routing ipv6 te forwarding statistics

Old syntax

reset segment-routing ipv6 te forwarding statistics

New syntax

reset segment-routing ipv6 te forwarding statistics [**binding-sid** *binding-sid* | **color** *color-value* **endpoint** *endpoint-ipv6* | **name** *name-value*]

Views

User view

Change description

The following parameters are added:

binding-sid *bsid*: Specifies the BSID of an SRv6 TE policy, which is an IPv6 address.

color *color-value* **endpoint** *endpoint-ipv6*: Specifies the color value and end-point IPv6 address of an SRv6 TE policy. The value range for the *color-value* argument is 0 to 4294967295.

name *policy-name*: Specifies the name of an SRv6 TE policy, a case-sensitive string of 1 to 59 characters.

Modified feature: Enabling Router ID filtering

Feature change description

As from this version, the **router-id filter** command supports the **bgp-rib-only** keyword.

Command reference

Modified command: router-id filter

Use **router-id filter** to enable Router ID filtering.

Use **undo router-id filter** to disable Router ID filtering.

Old syntax

router-id filter

undo router-id filter

New syntax

router-id filter [**bgp-rib-only**]

undo router-id filter

Views

BGP IPv6 SR policy address family

Change description

The **bgp-rib-only** keyword is added.

bgp-rib-only: Enables the device to accept the route without generating an SRv6 TE policy accordingly when it receives a BGP IPv6 SR policy route and the Route Target attribute of the route does not carry the local router ID.

This command enables the device to check the Route Target attribute of a received BGP IPv6 SR policy route.

- If the Route Target attribute contains the Router ID of the local device, the device accepts the route and generates an SRv6 TE policy accordingly.
- If the Route Target attribute does not contain the Router ID of the local device, the device processes the route as follows:
 - If the **bgp-rib-only** keyword is not specified in the command, the device drops the route.
 - If the **bgp-rib-only** keyword is specified in the command, the device accepts the route but does not generate the corresponding SRv6 TE policy.

Modified feature: Support of the ipv6 route-static command for the gateway keyword

Feature change description

As from this release, the **ipv6 route-static** command supports the **gateway** keyword.

Command changes

Modified command: ipv6 route-static

Use **ipv6 route-static** to configure an IPv6 static route.

Use **undo ipv6 route-static** to remove an IPv6 static route.

Old syntax

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number
[ next-hop-address ] [ bfd { { control-packet | echo-packet } [ bfd-source ipv6-address ]
| static session-name } | permanent | track track-entry-number ] | [ vpn-instance
d-vpn-instance-name ] next-hop-address [ bfd { control-packet bfd-source ipv6-address |
static session-name } | permanent | track track-entry-number ] } [ preference preference ]
[ tag tag-value ] [ description text ]
```

```
undo ipv6 route-static ipv6-address prefix-length [ interface-type interface-number
[ next-hop-address ] | [ vpn-instance d-vpn-instance-name ] next-hop-address ]
[ preference preference ]
```

```

ipv6 route-static ipv6-address prefix-length srv6-policy { color color-value end-point ipv6
ipv6-address | name policy-name } [ sid sid ] [ preference preference ] [ tag tag-value ]
[ description text ]

```

```

undo ipv6 route-static ipv6-address prefix-length [ srv6-policy { color color-value
end-point ipv6 ipv6-address | name policy-name } ]

```

```

ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length
{ interface-type interface-number [ next-hop-address ] [ bfd { { control-packet |
echo-packet } [ bfd-source ipv6-address ] | static session-name } | permanent | track
track-entry-number ] | next-hop-address [ public ] [ bfd { control-packet bfd-source
ipv6-address | static session-name } | permanent ] | vpn-instance d-vpn-instance-name
next-hop-address [ bfd { control-packet bfd-source ipv6-address | static session-name } |
permanent | track track-entry-number ] } [ preference preference ] [ tag tag-value ]
[ description text ]

```

```

undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length
[ interface-type interface-number [ next-hop-address ] | next-hop-address [ public ] |
vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference ]

```

```

ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length srv6-policy
{ color color-value end-point ipv6 ipv6-address | name policy-name } [ sid sid ]
[ preference preference ] [ tag tag-value ] [ description text ]

```

```

undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length
[ srv6-policy { color color-value end-point ipv6 ipv6-address | name policy-name } ]

```

New syntax

```

ipv6 route-static ipv6-address prefix-length { interface-type interface-number
[ next-hop-address ] [ bfd { { control-packet | echo-packet } [ bfd-source ipv6-address ]
| static session-name } | permanent | track track-entry-number ] | [ vpn-instance
d-vpn-instance-name ] next-hop-address [ bfd { control-packet bfd-source ipv6-address |
static session-name } | permanent | track track-entry-number ] } [ preference preference ]
[ tag tag-value ] [ description text ]

```

```

ipv6 route-static ipv6-address prefix-length interface-type interface-number gateway [ bfd
{ { control-packet | echo-packet } [ bfd-source ipv6-address ] | static session-name } |
track track-entry-number ] [ preference preference ] [ tag tag-value ] [ description text ]

```

```

undo ipv6 route-static ipv6-address prefix-length [ interface-type interface-number
[ next-hop-address | gateway ] | [ vpn-instance d-vpn-instance-name ] next-hop-address ]
[ preference preference ]

```

```

ipv6 route-static ipv6-address prefix-length srv6-policy { color color-value end-point ipv6
ipv6-address | name policy-name } [ sid sid ] [ preference preference ] [ tag tag-value ]
[ description text ]

```

```

undo ipv6 route-static ipv6-address prefix-length [ srv6-policy { color color-value
end-point ipv6 ipv6-address | name policy-name } ]

```

```

ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length
{ interface-type interface-number [ next-hop-address ] [ bfd { { control-packet |
echo-packet } [ bfd-source ipv6-address ] | static session-name } | permanent | track
track-entry-number ] | next-hop-address [ public ] [ bfd { control-packet bfd-source
ipv6-address | static session-name } | permanent ] | vpn-instance d-vpn-instance-name
next-hop-address [ bfd { control-packet bfd-source ipv6-address | static session-name } |
permanent | track track-entry-number ] } [ preference preference ] [ tag tag-value ]
[ description text ]

```



```
ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length interface-type
interface-number gateway [ bfd { { control-packet | echo-packet } [ bfd-source
ipv6-address ] | static session-name } | track track-entry-number ]
```

```
undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length
[ interface-type interface-number [ next-hop-address | gateway ] | next-hop-address
[ public ] | vpn-instance d-vpn-instance-name next-hop-address ] [ preference
preference ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length srv6-policy
{ color color-value end-point ipv6 ipv6-address | name policy-name } [ sid sid ]
[ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length
[ srv6-policy { color color-value end-point ipv6 ipv6-address | name policy-name } ]
```

Views

System view

Change description

Before modification: The command does not support the **gateway** keyword.

After modification: The command supports the **gateway** keyword.

gateway: Specifies the next hop IPv6 address of the IPv6 static route as the gateway address obtained by the interface in IPv6 address autoconfiguration. When the gateway address changes, the device automatically updates the next hop IPv6 address of the IPv6 static route accordingly. For more information about IPv6 address autoconfiguration, see IPv6 basics and DHCPv6 in *Layer 3—IP Services Configuration Guide*.

New feature: License installation and AC configuration

Feature description

The device supports fast configuration of device license installation. On the device license installation page, you can perform the following tasks:

- View the remaining validity of a license and renew licenses in time.
- Install new licenses to unlock more functions.
- Upgrade the signature library to manage user online behavior.

The device supports fast configuration of ACs. On the wireless AC page, you can configure the SSID, client authentication method, and password. After you configure basic AC settings, wireless clients can access the Internet through the WLAN.

New feature: Configuring bandwidth guaranteeing

Feature description

You can configure this feature to guarantee bandwidth for specific users when congestion occurs.

New feature: Enabling NetStream sampling for an SRv6 TE policy

Enabling NetStream sampling for an SRv6 TE policy

About this task

During statistic collection about the outgoing traffic forwarded on the ingress node for an SRv6 TE policy, the device performance will decrease if the number of packets to be collected is too large. In this case, perform this task on the ingress node for the SRv6 TE policy to enable NetStream to sample the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Restrictions and guidelines

Perform this task on the ingress node for an SRv6 TE policy. This task does not take effect on any other nodes.

Procedure

1. Enter system view.
system-view
2. Create a sampler.
For more information about a sampler, see "Configuring samplers."
3. Enable NetStream sampling for an SRv6 TE policy.
ip netstream outbound sampler *sampler-name* srv6-policy end-point ipv6 *ipv6-address* color *color-value*
By default, NetStream sampling is disabled for an SRv6 TE policy.

Command reference

New command: ip netstream outbound sampler srv6-policy

Use **ip netstream outbound sampler srv6-policy** to enable NetStream sampling for an SRv6 TE policy.

Use **undo ip netstream outbound sampler srv6-policy** to disable NetStream sampling for an SRv6 TE policy.

Syntax

```
ip netstream outbound sampler sampler-name srv6-policy end-point ipv6 ipv6-address color color-value  
undo ip netstream outbound sampler sampler-name srv6-policy end-point ipv6 ipv6-address color color-value
```

Default

NetStream sampling is disabled for an SRv6 TE policy.

Views

System view

Predefined user roles

network-admin

Parameters

sampler-name: Specifies a sampler by its name. The name is a case-insensitive string of 1 to 31 characters. For more information about a sampler, see "Configuring samplers".

end-point ipv6 *ipv6-address*: Specifies the IPv6 address of the destination node for an SRv6 TE policy.

color *color-value*: Specifies the color for an SRv6 TE policy, in the range of 0 to 4294967295.

Usage guidelines

Execute this command on the ingress node for an SRv6 TE policy. This command does not take effect on any other nodes.

During the statistics collection about the outgoing traffic forwarded on the ingress node for an SRv6 TE policy, the device performance will decrease if the number of packets to be collected is too large. In this case, execute this command on the ingress node for the SRv6 TE policy to enable NetStream to sample the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Examples

Enable NetStream sampling by using sampler **abc** for the SRv6 TE policy whose destination node is at 1000::1 and color is 10.

```
<Sysname> system-view
```

```
[Sysname] ip netstream outbound sampler abc srv6-policy endpoint ipv6 1000::1 color 10
```

New feature: Enabling NetStream for an SRv6 TE policy

Enabling NetStream for an SRv6 TE policy

About this task

Perform this task on the ingress node for an SRv6 TE policy to enable NetStream to collect statistics about the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Restrictions and guidelines

Perform this task on the ingress node for an SRv6 TE policy. This task does not take effect on any other nodes.

Procedure

1. Enter system view.

system-view

2. Enable NetStream for an SRv6 TE policy.

ip netstream outbound srv6-policy end-point ipv6 *ipv6-address* color *color-value*

By default, NetStream is disabled for an SRv6 TE policy.

Command reference

New command: `ip netstream outbound srv6-policy`

Use **`ip netstream outbound srv6-policy`** to enable NetStream for an SRv6 TE policy.

Use **`undo ip netstream outbound srv6-policy`** to disable NetStream for an SRv6 TE policy.

Syntax

`ip netstream outbound srv6-policy end-point ipv6` *ipv6-address* **`color`** *color-value*

`undo ip netstream outbound srv6-policy end-point ipv6` *ipv6-address* **`color`** *color-value*

Default

NetStream is disabled for an SRv6 TE policy.

Views

System view

Predefined user roles

network-admin

Parameters

`end-point ipv6` *ipv6-address*: Specifies the IPv6 address of the destination node for an SRv6 TE policy.

`color` *color-value*: Specifies the color for an SRv6 TE policy, in the range of 0 to 4294967295.

Usage guidelines

Execute this command on the ingress node for an SRv6 TE policy. This command does not take effect on any other nodes.

This command enables NetStream to collect statistics about the outgoing traffic forwarded based on an SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Examples

```
# Enable NetStream for the SRv6 TE policy whose destination node is at 1000::1 and color is 10.
```

```
<Sysname> system-view
```

```
[Sysname] ip netstream outbound srv6-policy endpoint ipv6 1000::1 color 10
```

New feature: Enabling IPv6 NetStream sampling for an SRv6 TE policy

Enabling IPv6 NetStream sampling for an SRv6 TE policy

About this task

During statistic collection about the outgoing traffic forwarded on the ingress node for an SRv6 TE policy, the device performance will decrease if the number of packets to be collected is too large. In this case, perform this task on the ingress node for the SRv6 TE policy to enable IPv6 NetStream to

sample the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Restrictions and guidelines

Perform this task on the ingress node for an SRv6 TE policy. This task does not take effect on any other nodes.

Procedure

1. Enter system view.

system-view

2. Create a sampler.

For more information about a sampler, see "Configuring samplers."

3. Enable IPv6 NetStream sampling for an SRv6 TE policy.

ipv6 netstream outbound sampler *sampler-name* srv6-policy end-point ipv6 *ipv6-address* color *color-value*

By default, IPv6 NetStream sampling is disabled for an SRv6 TE policy.

Command reference

New command: ipv6 netstream outbound sampler srv6-policy

Use **ipv6 netstream outbound sampler srv6-policy** to enable IPv6 NetStream sampling for an SRv6 TE policy.

Use **undo ipv6 netstream outbound sampler srv6-policy** to disable IPv6 NetStream sampling for an SRv6 TE policy.

Syntax

ipv6 netstream outbound sampler *sampler-name* srv6-policy end-point ipv6 *ipv6-address* color *color-value*

undo ipv6 netstream outbound sampler *sampler-name* srv6-policy end-point ipv6 *ipv6-address* color *color-value*

Default

IPv6 NetStream sampling is disabled for an SRv6 TE policy.

Views

System view

Predefined user roles

network-admin

Parameters

sampler-name: Specifies a sampler by its name. The name is a case-insensitive string of 1 to 31 characters. For more information about a sampler, see *Network Management and Monitoring Configuration Guide*.

end-point ipv6 *ipv6-address*: Specifies the IPv6 address of the destination node for an SRv6 TE policy.

color *color-value*: Specifies the color for an SRv6 TE policy, in the range of 0 to 4294967295.

Usage guidelines

Execute this command on the ingress node for an SRv6 TE policy. This command does not take effect on any other nodes.

During the statistics collection about the outgoing traffic forwarded on the ingress node for an SRv6 TE policy, the device performance will decrease if the number of packets to be collected is too large. In this case, execute this command on the ingress node for the SRv6 TE policy to enable NetStream to sample the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Examples

```
# Enable IPv6 NetStream sampling by using sampler abc for the SRv6 TE policy whose destination node is at 1000::1 and color is 10.
```

```
<Sysname> system-view
```

```
[Sysname] ipv6 netstream outbound sampler abc srv6-policy endpoint ipv6 1000::1 color 10
```

New feature: Enabling IPv6 NetStream for an SRv6 TE policy

Enabling IPv6 NetStream for an SRv6 TE policy

About this task

Perform this task on the ingress node for an SRv6 TE policy to enable IPv6 NetStream to collect statistics about the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Restrictions and guidelines

Perform this task on the ingress node for an SRv6 TE policy. This task does not take effect on any other nodes.

Procedure

1. Enter system view.

```
system-view
```

2. Enable IPv6 NetStream for an SRv6 TE policy.

```
ipv6 netstream outbound srv6-policy end-point ipv6 ipv6-address color color-value
```

By default, IPv6 NetStream is disabled for an SRv6 TE policy.

Command reference

New command: **ipv6 netstream outbound srv6-policy**

Use **ipv6 netstream outbound srv6-policy** to enable IPv6 NetStream for an SRv6 TE policy.

Use **undo ipv6 netstream outbound srv6-policy** to disable IPv6 NetStream for an SRv6 TE policy.

Syntax

```
ipv6 netstream outbound srv6-policy end-point ipv6 ipv6-address color color-value
```

```
undo ipv6 netstream outbound srv6-policy end-point ipv6 ipv6-address color color-value
```

Default

IPv6 NetStream is disabled for an SRv6 TE policy.

Views

System view

Predefined user roles

network-admin

Parameters

end-point ipv6 *ipv6-address*: Specifies the IPv6 address of the destination node for an SRv6 TE policy.

color *color-value*: Specifies the color for an SRv6 TE policy, in the range of 0 to 4294967295.

Usage guidelines

Perform this task on the ingress node for an SRv6 TE policy. This task does not take effect on any other nodes.

This command enables IPv6 NetStream to collect statistics about the outgoing traffic forwarded based on that SRv6 TE policy. For more information about SRv6 TE policies, see *Segment Routing Configuration Guide*.

Examples

Enable IPv6 NetStream for the SRv6 TE policy whose destination node is at 1000::1 and color is 10.

```
<Sysname> system-view
```

```
[Sysname] ipv6 netstream outbound srv6-policy endpoint ipv6 1000::1 color 10
```

New feature: Importing the carrier address library at the GUI

Importing the carrier address library

As from this release, you can import the carrier address library file on the external network setting page at the GUI.

New feature: Configuring the time zone at the GUI

Configuring the time zone at the GUI

As from this release, you can synchronize the device time zone with that of the PC on the system settings page at the GUI. The device can automatically select the time zone of the Web access terminal.

New feature: Enabling Web logging

Enabling Web logging

After Web logging is enabled, operation logs are printed at the Web UI. You can view the log contents at the system log page.

Modified feature: Specifying multiple NTP servers

Feature change description

As a best practice, use automatic time synchronization if an NTP server is available in your network to provide more accurate time. With automatic time synchronization, the device uses the time obtained from the NTP server as the current system time and periodically synchronizes the time with the NTP server. The device can resynchronize the system time of the NTP server after it restarts.

Before modification:

To specify multiple NTP servers, navigate to the **System Tools > System Settings > Date/Time > Automatic time synchronization** page at the Web UI, enter the IP address of NTP server 1 for the **NTP Server 1** configuration item, and enter the IP address of NTP server 2 for the **NTP Server 2** configuration item.

After modification:

To specify multiple NTP servers, navigate to the **System Tools > System Settings > Date/Time > Automatic time synchronization** page at the Web UI, click **Default NTP Server List** and view the default NTP servers. To add an NTP server, enter the IP address or host name of that NTP server.

Modified feature: Flow-mirroring traffic to an interface

Feature change description

When you use syntax 1 to configure flow-mirroring traffic to an interface, packets are mirrored to the specified outgoing interface.

When you use syntax 2 to configure flow-mirroring traffic to an interface, the device first encapsulates the mirrored packets with the specified parameters. Then, the device looks up a route for the encapsulated mirrored packets based on their source IP address and destination IP address. The outgoing interface of the route is the destination interface of the mirrored packets. By configuring load sharing for the routing protocol, the mirrored packets can be sent to multiple destination interfaces. If a selected outgoing interface goes down, the device will send the mirrored packets out of another interface based on the routing metric recalculations.

Command changes

Modified command: mirror-to interface

Old syntax

```
mirror-to interface interface-type interface-number [ destination-ip destination-ip-address  
source-ip source-ip-address [ dscp dscp-value | vlan vlan-id | vrf-instance vrf-name ] * ]  
[ destination-mac mac-address ] ]  
  
undo mirror-to interface interface-type interface-number
```

New syntax

Syntax 1:

```
mirror-to interface interface-type interface-number [ destination-ip destination-ip-address  
source-ip source-ip-address [ dscp dscp-value | erspan-id erspan-id-value | vlan vlan-id |  
vrf-instance vrf-name ] * ] [ destination-mac mac-address ] ]  
  
undo mirror-to interface interface-type interface-number
```

Syntax 2:

```
mirror-to interface { destination-ip destination-ip-address source-ip source-ip-address }  
[ dscp dscp-value | erspan-id erspan-id-value | dscp dscp-value | vlan vlan-id |  
vrf-instance vrf-name ] * [ destination-mac mac-address ]  
  
undo mirror-to interface { destination-ip destination-ip-address source-ip  
source-ip-address }
```

Views

Traffic behavior view

Change description

The **erspan-id** keyword was added, and a new syntax form was added.

New feature: EoGRE

Ethernet over GRE (EoGRE) is a tunneling protocol that can encapsulate the Ethernet protocol into a virtual point-to-point tunnel over an IP network. Ethernet frames are encapsulated at one tunnel end and de-encapsulated at the other tunnel end.

EoGRE supports EoGRE tunnel mode and EoGRE-in-UDP tunnel mode. Set the tunnel mode to EoGRE-in-UDP only if Layer 2 Ethernet packets are forwarded across a Layer 3 network with NAT traversal.

The EoGRE configuration includes the following:

- Creating an EoGRE tunnel.
- Mapping a VEB interface to the EoGRE tunnel interface and monitoring EoGRE information.

New feature: Configuring ARP attack detection on the Web interface

About this task

This feature enables the device to detect all online devices attacked to the specified interface and check conflicts between dynamic ARP entries and static ARP entries. Black entries represent static ARP entries, blue entries represent dynamic ARP entries, and red entries represent error ARP entries.

New feature: Configuring NAT address pools on the Web interface

About this task

With address pool-based NAT configured, the system selects an address from the pool as the translated address. Typically, an NAT address pool contains public IP addresses assigned by the service provider.

New feature: Configuring application services on the Web interface

About this task

Application services allow you to configure Domain Name System (DNS). DNS is a distributed database used by TCP/IP applications to translate domain names into IP addresses. The domain name-to-IP address mapping is called a DNS entry. DNS can be static or dynamic.

Static DNS

Static DNS (SDNS) allows you to manually create mappings between domain names and IP addresses. When you use a domain name to access a service (for example, a Web, mail, or FTP service), the system will look up the DNS cache for the IP address mapped to the domain name.

Dynamic DNS

Dynamic DNS (DDNS) can dynamically update the mappings between domain names and IP addresses for DNS servers.

In some scenarios, for example, the dial-up access scenario, a WAN interface is used to provide the Web, mail, or FTP service, and the interface IP address changes. To allow users to access the service through a fixed domain name, you can configure DDNS on the WAN interface. When the IP address of the WAN interface changes, the device automatically sends packets to the DDNS server to update the domain name-to-IP address mapping.

New feature: Configuring a PCE

Configuring a PCE

About this task

An LSR acts as a PCC if no PCE IP address is specified for it. It uses its LSR ID to communicate with PCEs. To configure the LSR as a PCE, perform this task.

Procedure

1. Enter system view.
system-view
2. Enter MPLS TE view or PCC view.
 - o Enter MPLS TE view.
mpls te
 - o Enter PCC view.
pce-client
3. Configure a PCE IP address.
pce address *ip-address*
By default, no PCE address is configured.
4. (Optional.) Enable the SR capability for the PCE device.
pce capability segment-routing
By default, a PCE device does not have the SR capability.
To establish an SR-capable stateful PCEP session, you need to enable the SR capability on both peers of the PCEP session.

Command reference

pce-client

Use **pce-client** to enable the PCC capability and enter PCC view.

Use **undo pce-client** to disable the PCC capability.

Syntax

pce-client

undo pce-client

Default

The PCC capability is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the PCC capability and enter PCC view.

```
<Sysname> system-view
[Sysname] pce-client
[Sysname-pcc]
```

pce capability segment-routing

Use **pce capability segment-routing** to enable the SR capability for a PCC device.

Use **undo pce capability segment-routing** to disable the SR capability for a PCC device.

Syntax

pce capability segment-routing

undo pce capability segment-routing

Default

A PCC device does not have the SR capability.

Views

MPLS TE view

PCC view

Predefined user roles

network-admin

Usage guidelines

To establish an SR-capable PCEP session, you need to enable the SR capability on both peers of the PCEP session. An SR-capable active PCEP session supports computation, report, delegation, and update of SR-based LSPs.

In the current software version, a PCE device does not have the segment routing capability.

You can execute this command in either the MPLS TE view or the PCC view.

Examples

```
# Enable the SR capability for the PCC device.
```

New feature: Configuring stateful PCE on a PCC

Configuring stateful PCE on a PCC

About this task

For a PCC and a PCE to establish a stateful PCEP session, you must specify the same device type (active stateful or passive stateful) for the two devices.

- If they are configured as passive-stateful devices, the PCE knows all CRLSPs maintained by the PCC but does not accept delegation requests sent by the PCC.
- If they are configured as active-stateful devices, the PCC can delegate CRLSPs to the PCE. If multiple PCEs are available for CRLSP delegation in the network, the PCC chooses the PCE with the highest delegation priority.

If a PCEP session between a PCC and a PCE terminates, the PCC waits for the redelegation timeout interval before it redelegates the CRLSP. If the PCEP session is re-established within the

relegation timeout interval, the PCC redelegates the CRLSP to the PCE. If the PCEP session fails to be re-established within the interval, the PCC redelegates the CRLSP to the PCE that has the second highest delegation priority.

If the redelegation fails and the CRLSP state timeout expires, the PCC uses the path calculated locally to establish the CRLSP.

If Segment Routing (SR) is used to establish tunnels, PCCs delegate SRLSPs to SR-capable PCEs, and establishes the SRLSPs by using the update messages sent by the PCEs. For more information about Segment Routing, see the SR-MPLS configuration in *Segment Routing Configuration Guide*.

If multi-delegation is enabled on a PCC, the PCC can delegate delegation-enabled dynamic CRLSPs and SRLSPs to all the PCEs specified for the PCC. The PCC updates the CRLSPs and SRLSPs according to the update requests received from any of the PCEs.

Restrictions and guidelines

The CRLSP state timeout interval must be greater than or equal to the redelegation timeout interval.

To use SR to establish a tunnel, you must enable the SR capability on the active stateful PCEP devices (by using the **pce capability segment-routing** command).

Enabling delegation

1. Enter system view.
system-view
2. Enter MPLS TE view or PCC view.
 - o Enter MPLS TE view.
mpls te
 - o Enter PCC view.
pce-client
3. Configure the PCEP device type as active stateful or passive stateful.
pcep type { active-stateful | passive-stateful }
By default, the PCEP device type is stateless.
4. (Optional.) Enable the multi-delegation feature on the PCC to delegate CRLSPs and SRLSPs to all PCEs.
pce multi-delegate enable
By default, the multi-delegation feature is disabled.
5. (Optional.) Enable the SR capability of the PCEP device.
pce capability segment-routing
By default, the device does not have the SR capability.
To establish an SR-capable stateful PCEP session, enable the SR capability on both peers of the session.
6. Return to system view.
quit
7. Enter MPLS TE tunnel interface view.
interface tunnel tunnel-number [mode mpls-te]
8. Enable CRLSP delegation.
mpls te delegation
By default, CRLSP delegation is disabled.
9. (Optional.) Configure MPLS TE to use SR to establish the tunnel.
mpls te signaling segment-routing
By default, MPLS TE uses RSVP-TE to establish a tunnel.

Execute this command when SRLSP delegation is enabled.

Configuring delegation parameters

1. Enter system view.
system-view
2. Enter MPLS TE view or PCC view.
 - o Enter MPLS TE view.
mpls te
 - o Enter PCC view.
pce-client
3. Configure the PCEP device type as active stateful or passive stateful.
pcep type { active-stateful | passive-stateful }
By default, the PCEP device type is stateless.
4. Set the delegation priority of a PCE.
pce peer ip-address delegation-priority priority
By default, the delegation priority of a PCE is 65535.
A smaller value represents a higher priority.
5. Set the redelegation timeout interval.
pce redelegation-timeout value
By default, the redelegation timeout interval is 30 seconds.
6. Set the state timeout interval on the PCC.
pce state-timeout value
By default, the state timeout interval is 60 seconds.
7. (Optional.) Enable the SR capability.
pce capability segment-routing
By default, the device does not have the SR capability.
To establish an SR-capable stateful PCEP session, enable the SR capability on both peers of the session.
8. (Optional.) Configure the PCC to retain PCE-updated LSP states.
pce retain lsp-state
By default, a PCC restores the original LSP states when the state timeout interval expires.
9. (Optional.) Configure the PCC to retain PCE-initiated LSPs.
pce retain initiated-lsp
By default, a PCC deletes PCE-initiated LSPs when the state timeout interval expires.

Command reference

pce multi-delegate enable

Use **pce multi-delegate enable** to enable the multi-delegation feature on a PCC to delegate CRLSPs or SRLSPs to all PCEs.

Use **undo pce multi-delegate enable** to disable the multi-delegation feature.

Syntax

pce multi-delegate enable

undo pce multi-delegate enable

Default

The multi-delegation feature is disabled.

Views

MPLS TE view

PCC view

Predefined user roles

network-admin

Usage guidelines

If multi-delegation is enabled on a PCC, the PCC can delegate delegation-enabled dynamic CRLSPs and SRLSPs to all the PCEs that have established active-stateful PCEP sessions with the PCC. The PCC updates the CRLSPs and SRLSPs according to the update requests received from any of the PCEs.

You can execute this command in either the MPLS TE view or the PCC view.

Example

```
# Enable the PCC to delegate CRLSPs or SRLSPs to all its PCEs.
```

```
<Sysname> system-view
```

```
[Sysname] mpls te
```

```
[System-te] pce multi-delegate enable
```

Related commands

display mpls te pce peer

pce retain initiated-lsp

Use **pce retain initiated-lsp** to configure the PCC to retain PCE-initiated LSPs.

Use **undo pce retain initiated-lsp** to restore the default.

Syntax

pce retain initiated-lsp

undo pce retain initiated-lsp

Default

A PCC deletes PCE-initiated LSPs when the state timeout interval expires.

Views

MPLS TE view

PCC view

Predefined user roles

network-admin

Usage guidelines

After an active-stateful PCE establishes a connection with a PCC, the PCE can send an initiate message to the PCC to create an LSP. After the PCE is disconnected from the PCC, the PCC deletes the PCE-initiated LSPs when the state timeout interval (set by using the **pce state-timeout** command) expires. If the **pce retain initiated-lsp** command is executed, the PCC will retain these PCE-initiated LSPs.

You can execute this command in either the MPLS TE view or the PCC view.

Examples

Configure the PCC to retain PCE-initiated LSPs.

```
<Sysname> system-view
[Sysname] mpls te
[Sysname-te] pce retain initiated-lsp
```

Related commands

pce state-timeout

pce retain lsp-state

Use **pce retain lsp-state** to configure the PCC to retain PCE-updated LSP states.

Use **undo pce retain lsp-state** to restore the default.

Syntax

pce retain lsp-state

undo pce retain lsp-state

Default

A PCC restores the original LSP states (the states before PCE updates) when the state timeout interval expires.

Views

MPLS TE view

PCC view

Predefined user roles

network-admin

Usage guidelines

After an active-stateful PCE establishes a connection with a PCC, the PCE can update the states of the delegated LSPs on the PCC. After the PCE is disconnected from the PCC, the PCC sets the PCE-updated LSPs to their original states when the state timeout interval (set by using the **pce state-timeout** command) expires. If the **pce retain lsp-state** command is executed, the PCC will retain the updated states for the LSPs.

The **pce retain lsp-state** command does not take effect on PCE-initiated LSPs.

You can execute this command in either the MPLS TE view or the PCC view.

Examples

Configure the PCC to retain PCE-updated LSP states.

```
<Sysname> system-view
[Sysname] mpls te
[Sysname-te] pce retain lsp-state
```

Related commands

mpls te delegation

pce state-timeout

New feature: Configuring PCEP session parameters

Configuring PCEP session parameters

About this task

This task allows you to configure parameters for PCCs or PCEs to establish PCEP sessions to manually specified or dynamically discovered PCEs.

Procedure

1. Enter system view.
system-view
2. Enter MPLS TE view or PCC view.
 - o Enter MPLS TE view.
mpls te
 - o Enter PCC view.
pce-client
3. Set the path calculation request timeout time.
pce request-timeout *value*
By default, the request timeout time is 10 seconds.
4. Set the PCEP session deadtimer.
pce deadtimer *value*
By default, the PCEP session deadtimer is 120 seconds.
5. Set the keepalive interval for PCEP sessions.
pce keepalive *interval*
By default, the keepalive interval is 30 seconds.
6. Set the minimum acceptable keepalive interval and the maximum number of allowed unknown messages received from the peer.
pce tolerance { **min-keepalive** *value* | **max-unknown-messages** *value* }
By default, the minimum acceptable keepalive interval is 10 seconds, and the maximum number of allowed unknown messages in a minute is 5.
7. Configure PCEP session authentication for a peer. Choose one option as needed:
 - o Configure the keychain authentication.
pce peer *ip-address* **keychain** *keychain-name*
 - o Configure the MD5 authentication.
pce peer *ip-address* **md5** { **cipher** | **plain** } *string*

By default, PCEP session authentication is not configured.

For two devices to establish a PCEP session, you must configure the same authentication mode and specify the same key string on both devices.

Command reference

pce peer keychain

Use **pce peer keychain** to configure keychain authentication for the PCEP session with a peer PCC or PCE.

Use **undo pce peer keychain** to remove the keychain authentication configuration for a peer PCC or PCE.

Syntax

pce peer *ip-address* **keychain** *keychain-name*

undo pce peer *ip-address* **keychain**

Default

PCEP session authentication is not configured.

Views

MPLS TE view

PCC view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a PCC or PCE.

keychain-name: Specifies a keychain by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

For two devices to establish a PCEP session, you must configure keychain authentication and specify the same key string on both devices.

This command and the **pce peer md5** command are mutually exclusive. A PCEP session supports only one type of security authentication.

You can execute this command in either the MPLS TE view or the PCC view.

Examples

Configure the device to use keychain **test** for authentication with peer PCE or PCC 10.10.10.10.

```
<Sysname> system-view
```

```
[Sysname] mpls te
```

```
[Sysname-te] pce peer 10.10.10.10 keychain test
```

pce peer md5

Use **pce peer md5** to configure MD5 authentication for the PCEP session with a peer PCC or PCE.

Use **undo pce peer md5** to remove the MD5 authentication configuration for a peer PCC or PCE.

Syntax

pce peer *ip-address* **md5** { **cipher** | **plain** } *string*

undo pce peer *ip-address* **md5**

Default

PCEP session authentication is not configured.

Views

MPLS TE view

PCC view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a PCC or PCE.

cipher: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters.

Usage guidelines

For two devices to establish a PCEP session, you must configure MD5 authentication and specify the same key string on both devices.

This command and the **pce peer keychain** command are mutually exclusive. A PCEP session supports only one type of security authentication.

You can execute this command in either the MPLS TE view or the PCC view.

Examples

Configure the device to perform MD5 authentication with peer PCE or PCC 10.10.10.10. Set the authentication key as **test** in plain text.

```
<Sysname> system-view
```

```
[Sysname] mpls te
```

```
[Sysname-te] pce peer 10.10.10.10 md5 plain test
```

New feature: Displaying local PCEP session settings and stateful PCE peers information

Displaying local PCEP session settings and stateful PCE peers information

Use **display mpls te pce parameter** to display local PCEP session settings.

Use **display mpls te pce stateful neighbor** to display information about stateful PCE peers on a PCC.

Command reference

display mpls te pce parameter

Use **display mpls te pce parameter** to display local PCEP session settings.

Syntax

display mpls te pce parameter

Views

Any view

Predefined user roles

- network-admin
- network-operator

Examples

```
# Display local PCEP session settings.
<Sysname> display mpls te pce parameter
Public Parameters:
  Keepalive interval      : 30 sec           Recommended deadtimer: 120 sec
  Request timeout        : 50 sec
  Tolerance:
    Min keepalive interval      : 10 sec
    Max unknown messages       : 5/min
  Capability for Nonstop routing: Yes
  Nonstop routing state       : Ready
PCC Parameters:
  PCEP Type                : Active stateful
  Capability for Initiate    : Yes
  Capability for Segment-Routing: Yes
  Retain lsp-state          : Enable
  Retain initiated-lsp      : Enable
  Redelegatation timeout    : 30 sec
  State timeout             : 60 sec
PCE Parameters:
  PCEP Type                : Stateless
  PCE Address               : 1.1.1.8
  Capability for Segment-Routing: No
```

Table 77 Command output

Field	Description
Public Parameters	Public parameters, which take effect when the device operates as a PCC or PCE.
Keepalive interval	Locally configured keepalive interval, in seconds.
Recommended deadtimer	Locally configured recommended PCEP session hold time, in seconds.
Request timeout	Path computation request timeout, in seconds.
Tolerance	Tolerance of the local device to the messages received from the PCE

Field	Description
	peer.
Min keepalive interval	Locally acceptable minimum keepalive interval (in seconds) sent by the peer.
Max unknown messages	Locally acceptable maximum number of unknown messages sent by the peer in a second.
Capability for Nonstop routing	Whether the local device supports PCEP nonstop routing (NSR): • Yes. • No.
Nonstop routing state	PCEP NSR state: • Ready—PCEP NSR has backed PCEP session information from the active process to the standby process. An active/standby switchover occurred in this state does not affect the existing PCEP session. Data forwarding will be not interrupted. • Not Ready—PCEP NSR is backing PCEP session information from the active process to the standby process. An active/standby switchover occurred in this state might result in re-establishment of the PCEP session, so data forwarding cannot be guaranteed. • Not configured—PCEP NSR is not enabled.
PCC Parameters	PCC parameters, which take effect only when the device operates as a PCC.
PCEP Type	Type of the local PCEP session: • Stateless. • Passive stateful. • Active stateful. The PCEP session type finally used is negotiated by the two peers.
Capability for Initiate	Whether the local device supports establishing tunnels and LSPs through PCE Initiated-LSP packets: • Yes. • No.
Capability for Segment-Routing	Whether the local device supports PCE Segment Routing: • Yes—The local device supports establishing SR-TE tunnels by using the following methods: ○ PCE sends Update packets (delegation update). ○ PCE sends Initial packets (actively establish) ○ Sends SR-TE path computation requests to the PCE. • No—The local device does not support PCE Segment Routing.
Retain lsp-state	Whether to retain the PCE-updated LSP states after the active stateful PCEP session is broken: • Enable—Retains the PCE-updated LSP states. • Disable—Does not retain the PCE-updated LSP states but restores the LSP states prior to the update.
Retain initiated-lsp	Whether to retain the PCE-initiated LSPs after the active stateful PCEP session is broken: • Enable—Retains the PCE-initiated LSPs. • Disable—Does not retain the PCE-initiated LSPs.
Redelegation timeout	Redelegation wait time (in seconds) after the PCEP session is broken.
State timeout	PCC state aging time (in seconds) after the PCEP session is broken.

Field	Description
PCE Parameters	PCE parameters, which take effect only when the device operates as a PCE.
PCE Address	PCE address advertised by the device when it operates as a PCE.

display mpls te pce stateful neighbor

Use **display mpls te pce stateful neighbor** to display information about stateful PCE peers on a PCC.

Syntax

display mpls te pce stateful neighbor [*ip-address*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

ip-address: Specifies the IP address of a stateful PCE peer. If you do not specify this argument, the command displays information about all stateful PCE peers.

Examples

Display information about the stateful PCE peer at 2.2.2.8.

```
<Sysname> display mpls te pce stateful neighbor 2.2.2.8
Neighbor address: 2.2.2.8
Session type      : Active stateful
Delegation priority: 1000
Synchronization   : Finished
Redelegation timer : Active
```

Table 78 Command output

Field	Description
Neighbor address	IP address of the stateful PCE peer.
Session type	PCEP session type: - Passive stateful. - Active stateful.
Delegation priority	Delegation priority. A bigger value represents a higher priority.
Synchronization	Synchronization state with the peer: - Not started. - Synchronizing. - Finished.
Redelegation timer	Running state of the redelegation timer: - Started. - Not started.

Modified feature: Configuring a NAT port mapping

Feature change description

Navigate to the **Network > NAT Settings** page of the Web interface. On the NAT port mapping configuration page, the **Protocol Type** options were changed.

Before modification, the options for the **Protocol Type** field are TCP and UDP.

After modification, the options for the **Protocol Type** field are TCP, UDP, TCP+UDP, and Custom.

Modified feature: Enabling BFD for LSPs associated with an FEC

Feature change description

As from this version, the device supports enabling BFD for the following types of LSPs associated with an FEC:

- IS-IS SRLSP.
- LDP LSP.
- OSPF SRLSP.
- Static LSP.

Command changes

Modified command: mpls bfd (for LSP)

Old syntax

```
mpls bfd dest-addr mask-length nexthop nexthop-address [ discriminator local local-id remote remote-id | echo | ldp-fec | nil-fec ] [ template template-name ]
```

```
undo mpls bfd dest-addr mask-length nexthop nexthop-address
```

```
mpls bfd dest-addr mask-length [ echo | ldp-fec ] [ template template-name ]  
[ backup-path template template-name ]
```

```
undo mpls bfd dest-addr mask-length
```

New syntax

```
mpls bfd dest-addr mask-length nexthop nexthop-address [ discriminator local local-id remote remote-id [ isis-srlsp | ldp-lsp | ospf-srlsp | static-lsp ] | echo | ldp-fec | nil-fec ]  
[ template template-name ]
```

```
undo mpls bfd dest-addr mask-length nexthop nexthop-address
```

```
mpls bfd dest-addr mask-length [ echo | ldp-fec ] [ template template-name ]  
[ backup-path template template-name ]
```

undo mpls bfd *dest-addr mask-length*

Views

System view

Change description

The [**isis-srlsp** | **ldp-lsp** | **ospf-srlsp** | **static-lsp**] parameter was added. You can use it to specify the following types of LSPs associated with an FEC as needed:

- IS-IS SRLSP.
- LDP LSP.
- OSPF SRLSP.
- Static LSP.

Modified feature: Displaying LSP information

Feature change description

As from this version, the device supports displaying information about LSPs interconnecting SRv6 and MPLS.

Command changes

Modified command: display mpls lsp

Old syntax

```
display mpls lsp [ egress | in-label label-value | ingress | outgoing-interface interface-type interface-number | protocol { bgp | isis | ldp | local | ospf | rsvp-te [ p2mp ] | sr-te | static | static-cr } | transit ] [ vpn-instance vpn-instance-name ] [ ipv4-address mask-length | ipv6 [ ipv6-address prefix-length ] ] [ verbose ]
```

New syntax

```
display mpls lsp [ egress | in-label label-value | ingress | outgoing-interface interface-type interface-number | protocol { bgp | isis | ldp | local | ospf | rsvp-te [ p2mp ] | sr-te | static | static-cr } | transit ] [ vpn-instance vpn-instance-name ] [ ipv4-address mask-length | ipv6 [ ipv6-address prefix-length ] ] [ srv6-mpls-interworking ] [ verbose ]
```

Views

Any view

Change description

The **srv6-mpls-interworking** keyword is added.

srv6-mpls-interworking: Displays LSPs interconnecting SRv6 and MPLS.

Modified feature: Configuring a preferred tunnel in a tunnel policy

Feature change description

As from this version, a tunnel policy supports using an SR-MPLS TE policy as a preferred tunnel.

Command changes

Modified feature: preferred-path

Old syntax

```
preferred-path { srv6-policy { name srv6-policy-name | end-point ipv6 ipv6-address color color-value } | tunnel number | tunnel-bundle number }
```

```
undo preferred-path { srv6-policy { name srv6-policy-name | end-point ipv6 ipv6-address color color-value } | tunnel number | tunnel-bundle number }
```

New syntax

```
preferred-path { sr-policy { name sr-policy-name | end-point ipv4 ipv4-address color color-value } | srv6-policy { name srv6-policy-name | end-point ipv6 ipv6-address color color-value } | tunnel number | tunnel-bundle number }
```

```
undo preferred-path { sr-policy { name sr-policy-name | end-point ipv4 ipv4-address color color-value } | srv6-policy { name srv6-policy-name | end-point ipv6 ipv6-address color color-value } | tunnel number | tunnel-bundle number }
```

Views

Tunnel policy view

Change description

The following parameters are added:

sr-policy: Specifies an SR-MPLS TE policy as the preferred tunnel.

name *sr-policy-name*: Specifies an SR-MPLS TE policy by its name.

end-point ipv4 *ipv4-address* **color** *color-value*: Specifies an SR-MPLS TE policy by the destination node address and color value. The *ipv4-address* argument specifies the IPv4 address of the destination node. The *color-value* argument represents the color value.

Modified feature: Binding tunnels to a destination IP address in a tunnel policy

Feature change description

As from this version, a tunnel policy supports binding an SR-MPLS TE policy group to a destination address.

Command changes

Modified command: binding-destination

Old syntax

```
binding-destination dest-ipv6-address { srv6-policy group srv6-policy-group-id |  
srv6-policy { name policy-name | end-point ipv6 ipv6-address color color-value } }  
[ ignore-destination-check ] [ down-switch ]  
  
undo binding-destination dest-ipv6-address
```

New syntax

```
binding-destination dest-ipv4-address { sr-policy group sr-policy-group-id | te { tunnel  
number } &<1-n> } [ ignore-destination-check ] [ down-switch ]  
  
binding-destination dest-ipv6-address { srv6-policy group srv6-policy-group-id |  
srv6-policy { name policy-name | end-point ipv6 ipv6-address color color-value } }  
[ ignore-destination-check ] [ down-switch ]  
  
undo binding-destination { dest-ipv4-address | dest-ipv6-address [ srv6-policy group  
srv6-policy-group-id | srv6-policy { name policy-name | end-point ipv6 ipv6-address color  
color-value } ] }
```

Views

Tunnel policy view

Change description

The following command syntax was added to support binding an SR-MPLS TE policy group to a destination address:

```
binding-destination dest-ipv4-address { sr-policy group sr-policy-group-id | te { tunnel  
number } &<1-n> } [ ignore-destination-check ] [ down-switch ]
```

New feature: Reserving an MPLS TE tunnel for tunnel binding policies

Reserving an MPLS TE tunnel for tunnel binding policies

Use **mpls te reserved-for-binding** to reserve an MPLS TE tunnel for tunnel binding policies.

Command reference

mpls te reserved-for-binding

Use **mpls te reserved-for-binding** to reserve an MPLS TE tunnel for tunnel binding policies.

Use **undo mpls te reserved-for-binding** to restore the default.

Syntax

```
mpls te reserved-for-binding
undo mpls te reserved-for-binding
```

Default

An MPLS TE tunnel can be used by any tunnel policy implementation methods.

Views

Tunnel interface view

Predefined user roles

network-admin

Usage guidelines

If a VPN has high requirements on bandwidth, you can select TE tunnels for the VPN by applying a tunnel policy bound with TE tunnels to the VPN.

You must execute this command for an MPLS TE tunnel before the tunnel can be bound to a destination address in a tunnel policy.

After you execute this command for an MPLS TE tunnel, the tunnel can only be used as a bound tunnel of a tunnel policy. For more information about tunnel binding, see the **binding-destination** command.

Examples

```
# Reserve an MPLS TE tunnel for tunnel binding policies.
<Sysname> system-view
[Sysname] interface tunnel 10 mode mpls-te
[Sysname-Tunnel10] mpls te reserved-for-binding
```

Modified feature: Configuring one-to-one mappings on the Web interface

Feature change description

As from this release, the **Specify permitted destination IP addresses** option is added to the **Add NAT One-to-One Mapping** page.

Select **Specify permitted destination IP addresses** to perform NAT on packets with a matching destination IP address. If you do not select this option, NAT is performed on all packets.

In the **IP address/mask** field, enter IP address/mask items to specify destination IP addresses used for matching.

Modified feature: Support of configuring Option 82 on a VEB interface

Feature change description

As from this release, DHCP snooping supports configuring Option 82 on a VEB interface.

Hardware and feature compatibility

Hardware	Feature compatibility
MSR610	Yes
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	Yes
MSR810-SI, MSR810-LM-SI	Yes
MSR810-LMS-EA, MSR810-LME	Yes
MSR1004S-5G, MSR1004S-5G-CN	Yes
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	Yes
MSR2630	Yes
MSR3600-28, MSR3600-51	Yes
MSR3600-28-SI, MSR3600-51-SI	Yes
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	Yes
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	Yes
MSR3610-G, MSR3620-G	Yes
MSR3640-G	Yes
MSR3640-X1-HI	No

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes

MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	Yes
MSR2630-WiNet	Yes
MSR3600-28-WiNet	Yes
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	Feature compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	Yes
MSR2630-XS	Yes
MSR3600-28-XS	Yes
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	No

Hardware	Feature compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	Yes

Command changes

Modified command: dhcp snooping information circuit-id

Old syntax

In Layer 2 Ethernet interface view/Layer 2 aggregate interface view:

```

dhcp snooping information circuit-id { [ vlan vlan-id ] string circuit-id | { normal | verbose [ node-identifier { mac | sysname | user-defined node-identifier } ] } [ format { ascii | hex } ] }

```

```

undo dhcp snooping information circuit-id [ vlan vlan-id ]

```

New syntax

In Layer 2 Ethernet interface view/Layer 2 aggregate interface view:

```

dhcp snooping information circuit-id { [ vlan vlan-id ] string circuit-id | { normal | verbose [ node-identifier { mac | sysname | user-defined node-identifier } ] } [ format { ascii | hex } ] }

```

```

undo dhcp snooping information circuit-id [ vlan vlan-id ]

```

In virtual Ethernet bridge (VEB) interface view:

```

dhcp snooping information circuit-id wlan-private [ encoded ] [ apmac apmac | bssid bssid | ssid ssid ] * [ format { ascii | hex } ]

```

```

undo dhcp snooping information circuit-id

```

Change description

After modification, the **dhcp snooping information circuit-id wlan-private** is supported in VEB interface view.

Parameters

- **wlan-private**: Specifies the WLAN-private mode. The padding content includes "WIRE", interface type and number, VLAN ID, SSID, BSSID, device name, and AP MAC address. For more information about SSID and BSSID, see WLAN access configuration in *WLAN Configuration Guide*.
- **encoded**: Transcodes the special characters padded to the **SSID**, **BSSID**, and **HOSTNAME** fields in the WLAN-private mode. Special characters include space, !, #, and \$. For example, you can transform the special characters padded to the **SSID**, **BSSID**, and **HOSTNAME** fields into hexadecimal values. If you do not specify this keyword, the device does not transcode the special characters padded to the **SSID**, **BSSID**, and **HOSTNAME** fields in the WLAN-private mode.
- **apmac** *apmac*: Specify an AP MAC address that is a 48-bit string of hexadecimal numbers in the format of HH:HH:HH:HH:HH:HH.
- **bssid** *bssid*: Specify a basic service set by its ID. A BSSID is a 48-bit string of hexadecimal numbers in the format of HH-HH-HH-HH-HH-HH.
- **ssid** *ssid*: Specify a service set by its ID. A SSID is a case-sensitive string of 1 to 32 characters.
- **format**: Specifies the padding format for the Circuit ID sub-option.
- **ascii**: Specifies the ASCII padding format.
- **hex**: Specifies the hex padding format.

The padding format varies by padding mode:

- If you do not specify any padding format, the padding format is ASCII in WLAN-private mode.
- If the specified padding format is ASCII, all contents will be padded in ASCII format.
- If the specified padding format is hex in WLAN-private mode, the VLAN ID, BSSID, and AP MAC address will be padded in hex format and other information will be padded in ASCII format.

Modified command: dhcp snooping information enable

Syntax

```

dhcp snooping information enable

```

undo dhcp snooping information enable

Old views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

New views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view
VEB interface view

Change description

After modification, this command is supported in VEB interface view.

Modified command: dhcp snooping information remote-id

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*]
 { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

Old views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view
VEB interface view

New views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view
VEB interface view

Change description

After modification, this command is supported in VEB interface view.

Modified command: dhcp snooping information strategy

Syntax

dhcp snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

Old views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

New views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

VEB interface view

Change description

After modification, this command is supported in VEB interface view.

Modified feature: Configuring a private address-to-public address mapping for an NHS of mGRE

Feature change description

As from this version, mGRE supports specifying the public DNS name of an NHRP server (NHS) instead of specifying its the public address.

Command changes

Modified command: `nhrp nhs`

Old syntax

```
nhrp nhs nhs-address nbma nbma-address  
undo nhrp nhs nhs-address nbma nbma-address
```

New syntax

```
nhrp nhs nhs-address nbma { dns-name | nbma-address }  
undo nhrp nhs nhs-address nbma { dns-name | nbma-address }
```

Views

mGRE tunnel interface view

Change description

The *dns-name* argument is added.

dns-name: Specifies the public DNS name of the NHS, a case-sensitive string of 1 to 253 characters. The string cannot contain a space.

Modified feature: Support for configuring Web Cache for devices in the RIR-SDWAN scenario

Feature change description

As from this release, you can configure Web Cache for devices in the RIR-SDWAN scenario.

Before modification: Devices in the RIR-SDWAN scenario do not support configuring Web Cache.

After modification: Devices in the RIR-SDWAN scenario support configuring Web Cache.

New feature: Configuring optimized features for HTTP proxy

About HTTP proxy

The HTTP proxy feature enables IPv6 clients to access IPv4 Web servers during network transition from IPv4 to IPv6. This feature has the following advantages:

- Simplifies smooth IPv4-to-IPv6 transition without affecting existing IPv4 services.
- Enables clients of one IP stack to access webpages of another IP stack, providing network compatibility and scalability.
- Supports load balancing, which improves the network efficiency and stability and enhances user experience.

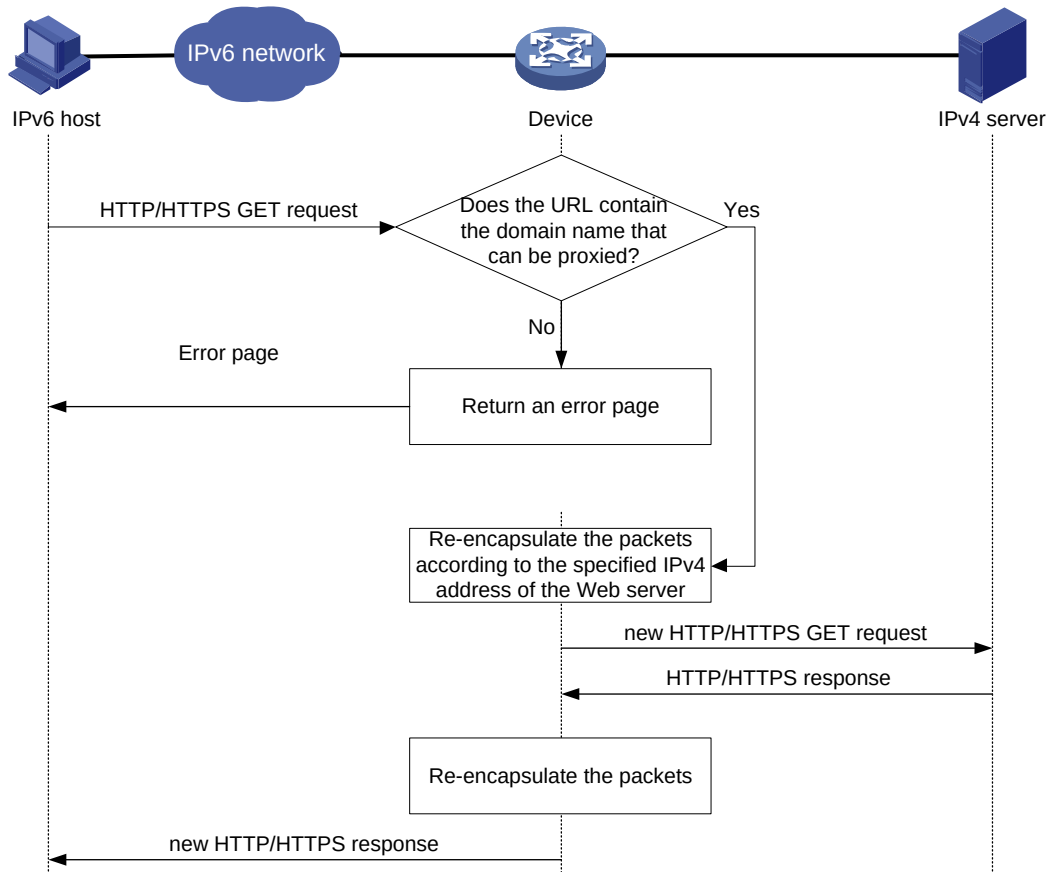
Working mechanism

The working mechanism of the HTTP proxy feature varies by the applicable scenarios.

- To proxy the HTTP or HTTPS requests to Web servers that provide the same service, you can specify the IPv4 addresses of Web servers for an HTTP proxy service. The Web servers in a Web server group provide load balancing.
- To proxy the HTTP or HTTPS requests to Web servers that provide different services, you can specify a DNS server to resolve the IPv4 addresses of Web servers for an HTTP proxy service.

HTTP proxy mechanism by using the specified IPv4 address of a Web server

Figure 42 HTTP proxy mechanism by using the specified IPv4 address of a Web server



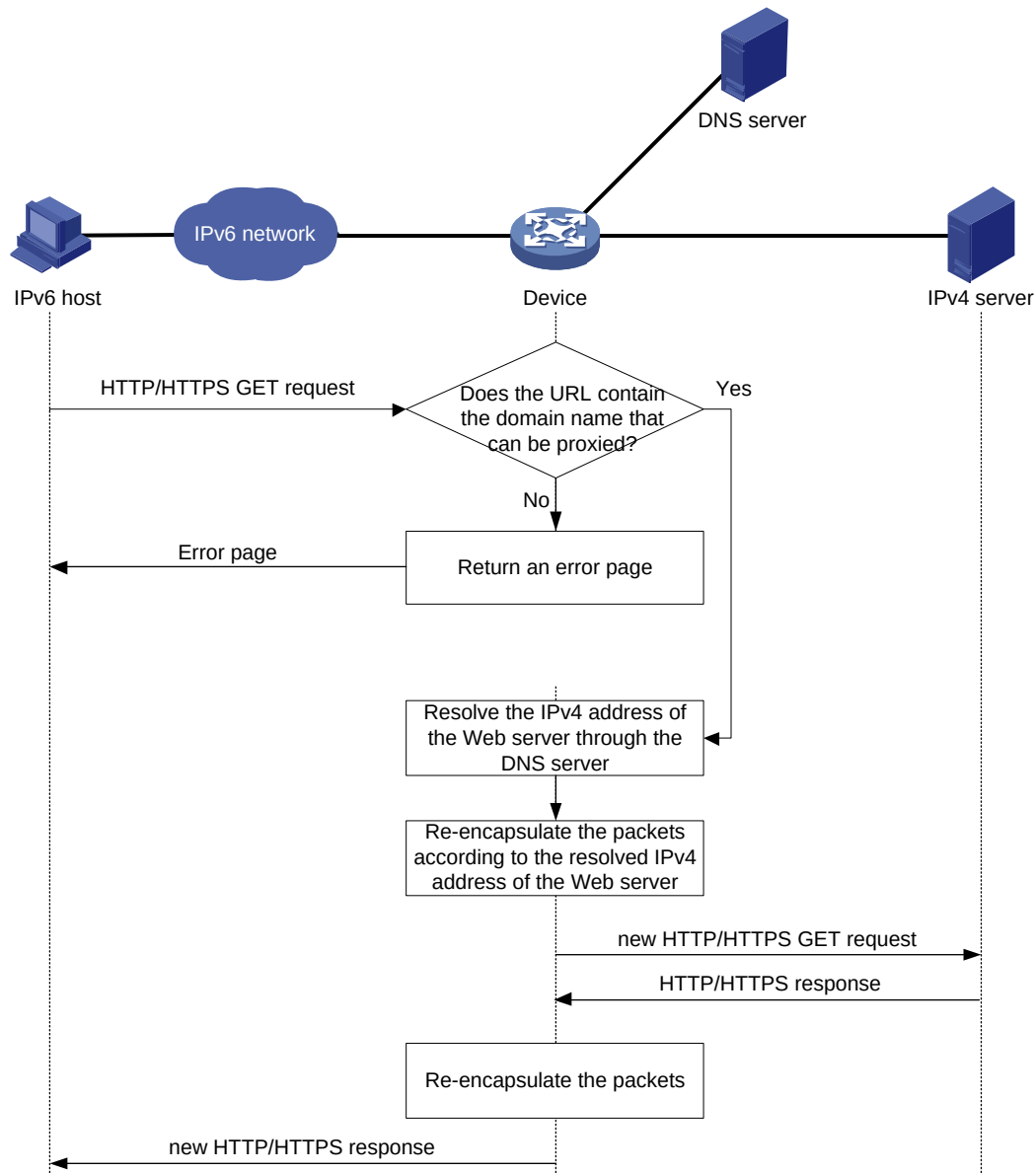
2. The IPv6 host obtains the IPv6 address corresponding to the requested domain name through a DNS server. The obtained IPv6 address is the IPv6 address of an HTTP proxy service configured on the device. The IPv6 host sends an HTTP or HTTPS GET request to the device.
3. The device checks whether the URL of the request contains the domain name that can be proxied by the HTTP proxy service:
 - If not, the device returns an error page to the IPv6 host.
 - If yes, the device takes the subsequent steps.

By default, the device can proxy all domain names. With denylist domain names specified on the device, the device cannot proxy the requests to the Web servers that use the specified denylist domain names. With allowlist domain names specified on the device, the device can only proxy the requests to the Web servers that use the specified allowlist domain names.

4. The device re-encapsulates the HTTP or HTTPS GET request according to the specified IPv4 address of the Web server and sends the new request to the IPv4 Web server.
5. The IPv4 Web server sends an HTTP or HTTPS response to the device.
6. The device re-encapsulates the HTTP or HTTPS response and sends it to the IPv6 host.

HTTP proxy mechanism by using the resolved IPv4 address of a Web server

Figure 43 HTTP proxy mechanism by using the resolved IPv4 address of a Web server



2. The IPv6 host obtains the IPv6 address corresponding to the requested domain name through a DNS server. The obtained IPv6 address is the IPv6 address of an HTTP proxy service configured on the device. The IPv6 host sends an HTTP or HTTPS GET request to the device.
3. The device checks whether the URL of the request contains the domain name that can be proxied by the HTTP proxy service:
 - If not, the device returns an error page to the IPv6 host.
 - If yes, the device obtains the IPv4 address of the Web server through the DNS server, re-encapsulates the HTTP or HTTPS GET request according to the resolved IPv4 address of the Web server, and sends the new request to the IPv4 Web server.

By default, the device can proxy all domain names. With denylist domain names specified on the device, the device cannot proxy the requests to the Web servers that use the specified denylist domain names. With allowlist domain names specified on the device, the device can only proxy the requests to the Web servers that use the specified allowlist domain names.

4. The IPv4 Web server sends an HTTP or HTTPS response to the device.
5. The device re-encapsulates the HTTP or HTTPS response and sends it to the IPv6 host.

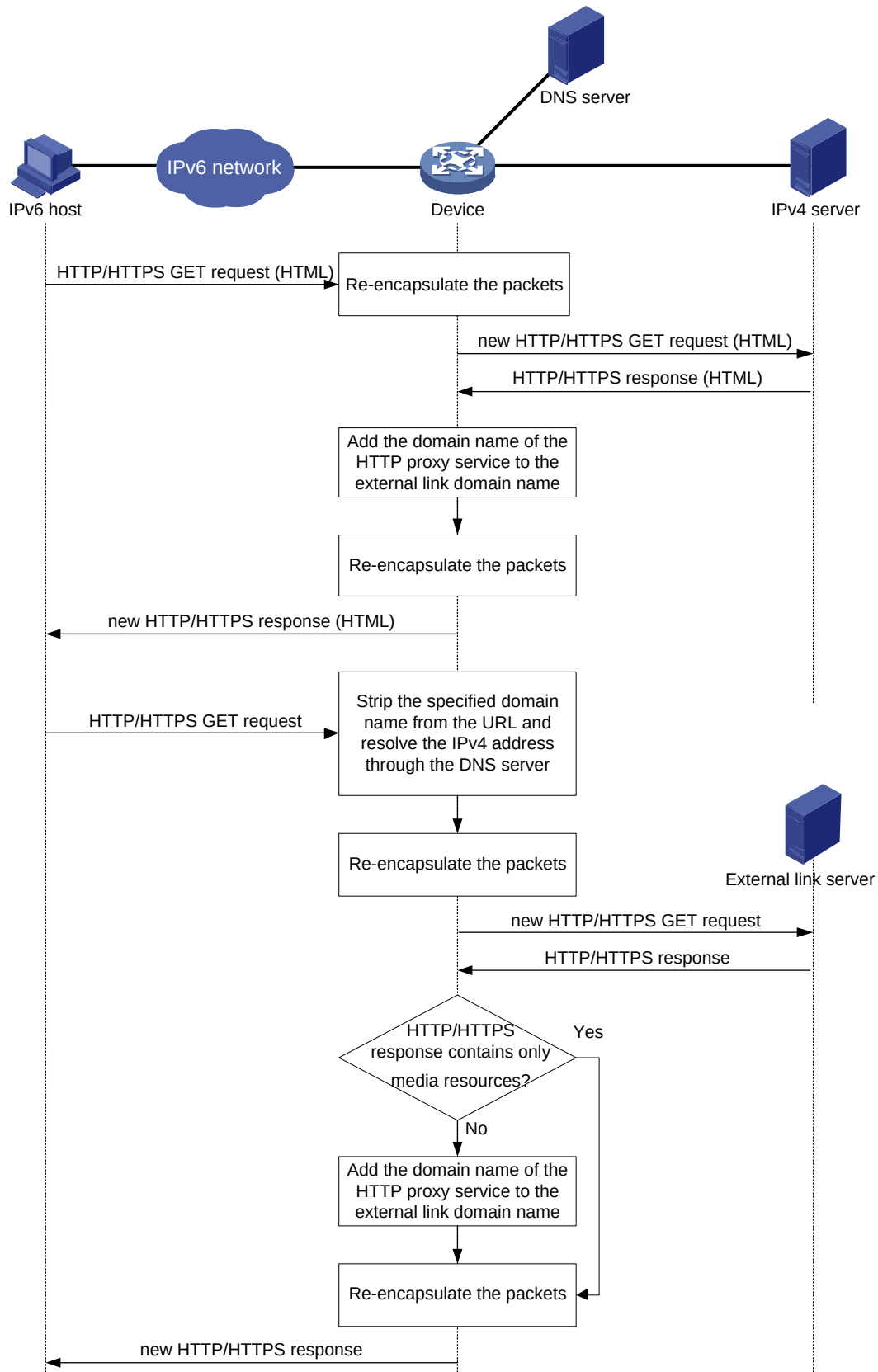
External link proxy

An external link is a hyperlink that exists on the webpages of an IPv4 server accessed by a client and is used to redirect to other websites.

By default, the IPv6 clients cannot access the external links on the webpages of an IPv4 server. Thus, you need to configure the external link proxy feature.

错误!未找到引用源。 shows the mechanism of external link proxy when an IPv6 client accesses external links on webpages of the IPv4 Web server.

Figure 44 External link proxy mechanism



2. The IPv6 host requests the HTML resource of the Web server. The IPv6 host obtains the IPv6 address corresponding to the requested domain name through a DNS server. The obtained

IPv6 address is the IPv6 address of an HTTP proxy service configured on the device. The IPv6 host sends an HTTP or HTTPS GET request to the device.

3. The device re-encapsulates the HTTP or HTTPS GET request and sends the new request to the IPv4 Web server.
4. The Web server encapsulates the data containing the HTML resource in the HTTP or HTTPS response and sends the response to the device.
5. Upon receiving the HTTP or HTTPS response, the device adds the domain name specified for the HTTP proxy service to the external link domain name and sends the new response to the client.

The specified domain name for the HTTP proxy service can be an allowlist domain name or a wildcard domain name. If you use the wildcard domain name for the HTTP proxy service, you must enable external link reference. Thus, all external links can be proxied.

6. When the IPv6 host accesses an external link on the webpages of the IPv4 server, the DNS server resolves the domain name in the request to the IPv6 address of the HTTP proxy service. The IPv6 host sends an HTTP or HTTPS request for an external link to the device.
7. Upon receiving the HTTP or HTTPS request for an external link, the device strips the domain name from the URL of the request.
8. The device resolves the domain name to the IPv4 address of the request through the DNS server.
9. The device re-encapsulates the request according to the resolved IPv4 address and sends the request to the external link server.
10. The external link server encapsulates the media resources and HTML resources in the HTTP or HTTPS response and sends the response to the device.
11. If the response contains only the media resources, the device directly re-encapsulates the response and sends the response to the IPv6 host. Otherwise, the device adds the domain name specified for the HTTP proxy service to the response that contains the external link, re-encapsulates the response, and sends the response to the IPv6 host.

License requirement for HTTP proxy

The HTTP proxy feature requires a license. If you configure the feature without a license, the settings will be lost after a device reboot. For information about license management, see *Fundamentals Configuration Guide*.

HTTP proxy tasks at a glance

To configure HTTP proxy in an HTTP proxy service view, perform the following tasks:

1. (Optional.) [错误!未找到引用源。](#)
2. [错误!未找到引用源。](#)
3. [Specifying an SSL certificate file and SSL certificate key file](#)
 - [Specifying an SSL certificate file and SSL certificate key file](#)
 - [Specifying a domain-specific SSL certificate file and SSL certificate key file](#)To enable the device to proxy HTTPS requests, you must perform this task.
4. (Optional.) [Configuring the external link proxy feature](#)
 - [Configuring the external media link proxy feature](#)
 - [Configuring the external hyperlink proxy feature](#)
 - [Configuring the external link reference feature](#)
5. (Optional.) [Configuring the advanced features for an HTTP proxy service](#)

- Configuring a source IP pool used for Web server connection
 - Enabling caching of Web server resources
 - Specifying a keyword to be monitored and a keyword to replace the monitored keyword
 - Enabling referer protection
 - Enabling URL protection
6. Enabling an HTTP proxy service
 7. (Optional.) 错误!未找到引用源。

Configuring a Web server group

About this task

You can add multiple IPv4 Web servers to a Web server group for an HTTP proxy service and bind the group to the HTTP proxy service. When the device receives HTTP or HTTPS requests, it distributes the traffic to different Web servers according to a certain algorithm, implementing load balancing. This increases network bandwidth and improves network availability and flexibility.

To proxy both HTTP and HTTPS packets, you can bind a Web server group specified with HTTP and a Web server group specified with HTTPS to an HTTP proxy service.

To implement load balancing, you can add multiple IPv4 Web servers with different IP addresses and port numbers to an IPv4 Web server group.

Restrictions and guidelines

With this feature configured, the device can only send the HTTP or HTTPS requests to the specified Web servers. If an IPv6 client accesses a Web server that is not configured on the device, the device will return an error page to the client.

Before binding a Web server group to an HTTP proxy service, first configure the parameters of the Web server group.

To modify the parameters of a Web server group that has been bound to an HTTP proxy service, first unbind the Web server group from the HTTP proxy service. Then, modify the parameters of the Web server group.

Make sure the protocol types of the all Web servers in a Web server group are consistent with the protocol type of the Web server group.

Procedure

1. Enter system view.
system-view
2. Create a Web server group and enter its view.
http-proxy server-group *group-name*
3. Add a Web server to the Web server group.
ip-address *ip-address* [**port** *port-number*]
By default, no Web servers exist in a Web server group.
4. Specify a protocol type for the Web server group.
protocol-type { **http** | **https** }
By default, no protocol types are specified for a Web server group.

Configuring an HTTP proxy service

About this task

An HTTP proxy service listens for and proxies HTTP or HTTPS requests from a specified TCP port number and IPv6 address. To proxy HTTPS packets, you must also specify an SSL certificate file and SSL certificate key file so the device can establish secure connections to IPv6 clients.

Upon receiving an HTTP or HTTPS request, the device checks whether the URL of request can be proxied by an HTTP proxy service. You can configure denylist domain names and allowlist domain names for an HTTP proxy service to filter the domain names. By default, the device can proxy all reachable domain names that can be resolved into reachable IPv4 addresses through a DNS server or proxy the specified domain names for Web server groups. To allow the device to proxy only the specified domain names, configure the specified domain names as allowlist domain names. To prevent the device from proxy the specified domain names, configure the specified domain names as denylist domain names.

Restrictions and guidelines

The protocol type of an HTTP proxy service can be different from the protocol type of the Web server group bound to the HTTP proxy service.

When configuring allowlist domain names and denylist domain names, obey the following rules:

- A domain name can only be configured as an allowlist domain name or a denylist domain name. The **denylist-domain-name** and **domain-name** commands are mutually exclusive.
- An HTTP proxy service supports a maximum of 512 denylist domain names and 512 allowlist domain names.
- Do not configure the allowlist domain names and denylist domain names at the same time.

Prerequisites

You must specify an unused TCP port number for an HTTP proxy service. To view TCP port numbers in use, execute the **display tcp** command.

To modify the parameters of an enabled HTTP proxy service, first disable the HTTP proxy service.

Procedure

1. Enter system view.
system-view
2. Create an HTTP proxy service and enter its view.
Centralized devices:
http-proxy service service-name
Distributed devices in standalone mode: Centralized IRF devices:
http-proxy service service-name slot slot-number
Distributed devices in IRF mode:
http-proxy service service-name chassis chassis-number slot slot-number
3. Specify a protocol type and listening port for the HTTP proxy service and bind a Web server group to the service.
protocol-type { http | https } [port port-number] [server-group group-name]
By default, no protocol type or listening port number is specified for an HTTP proxy service and no Web server group is bound to the HTTP proxy service.
4. Specify an IPv6 address for the HTTP proxy service.
ipv6-address ipv6-address
By default, no IPv6 address is specified for an HTTP proxy service.

5. (Optional.) Specify a DNS server for the HTTP proxy service.

dns-server *ip-address*

By default, no DNS servers are specified for an HTTP proxy service.

If you do not specify a Web server group for an HTTP proxy service, you must configure a DNS server for the HTTP proxy service.

6. Specify a domain name for the HTTP proxy service. Choose one option as needed:

- Specify a denylist domain name for the HTTP proxy service.

denylist-domain-name *denylist-domain-name*

- Specify an allowlist domain name for the HTTP proxy service.

domain-name *domain-name*

By default, no denylist domain names or allowlist domain names are specified for an HTTP proxy service.

Specifying an SSL certificate file and SSL certificate key file

About specifying an SSL certificate file and SSL certificate key file

After specifying a Web server group for an HTTP proxy service, you can specify an SSL certificate file and SSL certificate key file for the HTTP proxy service. Thus, the HTTP proxy service can handle the HTTPS requests for one domain name.

After specifying a DNS server for an HTTP proxy service, you can specify multiple pairs of SSL certificate files and SSL certificate key files for the HTTP proxy service. Thus, the HTTP proxy service can handle the HTTPS requests for different domain names.

Restrictions and guidelines

The **ssl certificate domain-name file key-file** command is mutually exclusive with the **ssl certificate file** command and the **ssl certificate key-file** command.

To allow an HTTP proxy service to proxy HTTP requests for multiple domain names, you can execute the **ssl certificate domain-name file key-file** command multiple times. Thus, the device can establish secure connections to IPv6 clients who request to access the web servers of different domain names.

Prerequisites

Before you execute the **ssl certificate file** and the **ssl certificate key-file** commands to specify an SSL certificate file and SSL certificate key file, upload the files to the device through FTP or TFTP. Before you execute the **ssl certificate domain-name file key-file** command to specify an SSL certificate file and SSL certificate key file, make sure the directory for storing the files exists and then upload the files to the device through FTP or TFTP. If the director for storing the SSL certificate file and SSL certificate key files does not exist, create a directory. For more information about FTP and TFTP configuration, see *Fundamentals Configuration Guide*.

Before specifying an SSL certificate file and SSL certificate key file for an HTTP proxy service, first disable the HTTP proxy service.

Specifying an SSL certificate file and SSL certificate key file

1. Enter system view.
system-view
2. Create an HTTP proxy service and enter its view.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode:Centralized IRF devices:
http-proxy service *service-name* **slot** *slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*
3. Specify an SSL certificate file.
ssl certificate file *certificate-file*
By default, no SSL certificate file is specified.
4. Specify an SSL certificate key file.
ssl certificate key-file *key-file*
By default, no SSL certificate key file is specified.

Specifying a domain-specific SSL certificate file and SSL certificate key file

1. Enter system view.
system-view
2. Create an HTTP proxy service and enter its view.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode:Centralized IRF devices:
http-proxy service *service-name* **slot** *slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*
3. Specify a directory to store SSL certificates and SSL certificate key files.
ssl certificate directory *directory*
By default, no directory is specified to store SSL certificates and SSL certificate key files.
4. Specify an SSL certificate file and SSL certificate key file for the HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.
ssl certificate domain-name *domain-name* **file** *certificate-file* **key-file** *key-file*
By default, no SSL certificate file and SSL certificate key file are specified for an HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.

Configuring the external link proxy feature

About configuring the external link proxy feature

For an HTTP proxy service, configure the external link proxy feature as required:

- The external media link proxy feature enables the IPv6 clients to access all external media resources (such as pictures or videos) on webpages of proxied Web servers. The proxied Web servers must use the domain names in the allowlist.
- The external hyperlink proxy feature enables the HTTP proxy service to proxy external hyperlinks on webpages of proxied Web servers by adding the specified domain name to the link URLs. The proxied Web servers must use the domain names in the allowlist. In this way, the clients can access webpage resources that are not on the proxied Web servers and the media resources on the accessed webpages.
- The external link reference feature enables the HTTP proxy service to proxy all external links on webpages of proxied Web servers by adding the wildcard domain name to the link URLs. In this way, the IPv6 clients can access the webpage resources and media resources on webpages of all Web servers. To configure the device to not proxy the requests for external links of a specific domain name, execute the **exclude-external-domain** command.

Prerequisites

Before configuring the external link proxy feature for an HTTP proxy service, first disable the HTTP proxy service.

Configuring the external media link proxy feature

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy service.
Centralized devices:
http-proxy service service-name
Distributed devices in standalone mode: Centralized IRF devices:
http-proxy service service-name slot slot-number
Distributed devices in IRF mode:
http-proxy service service-name chassis chassis-number slot slot-number
3. Specify an allowlist domain name for the HTTP proxy service.
domain-name domain-name
By default, no allowlist domain names are specified for an HTTP proxy service.
4. (Optional.) Specify a DNS server for the HTTP proxy service.
dns-server ip-address
By default, no DNS servers are specified for an HTTP proxy service.
If you do not specify a Web server group for an HTTP proxy service, you must configure a DNS server for the HTTP proxy service.
5. Enable the external media link proxy feature.
medialink-proxy enable
By default, the external media link proxy feature is disabled.

Configuring the external hyperlink proxy feature

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy service.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode:Centralized IRF devices:
http-proxy service *service-name slot slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name chassis chassis-number slot slot-number*
3. Specify an allowlist domain name for the HTTP proxy service.
domain-name *domain-name*
By default, no allowlist domain names are specified for an HTTP proxy service.
4. (Optional.) Specify a DNS server for the HTTP proxy service.
dns-server *ip-address*
By default, no DNS servers are specified for an HTTP proxy service.
If you do not specify a Web server group for an HTTP proxy service, you must configure a DNS server for the HTTP proxy service.
5. Specify an external hyperlink to be proxied on webpages.
hyperlink-proxy *link-string*
By default, no external hyperlinks are specified to be proxied.

Configuring the external link reference feature

Restrictions and guidelines

To make this feature take effect for an HTTP proxy service, you must specify a wildcard domain name for the HTTP proxy service.

With both a wildcard domain name and allowlist domain name configured for an HTTP proxy service, the HTTP proxy service adds only the wildcard domain name to the external link domain name.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy service.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode:Centralized IRF devices:
http-proxy service *service-name slot slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name chassis chassis-number slot slot-number*
3. Specify a wildcard domain name for the HTTP proxy service.
wildcard-domain-name *wildcard-domain-name*
By default, wildcard domain name **extlink.cn** is specified for an HTTP proxy service.
4. Enable external link reference for the HTTP proxy service.

extlink-href enable

By default, the external link reference feature for an HTTP proxy service is disabled.

5. (Optional.) Specify an external link domain name to be not proxied by the HTTP proxy service.

exclude-external-domain *domain-name*

By default, no external link domain names to be not proxied are specified for an HTTP proxy service.

Configuring the advanced features for an HTTP proxy service

Configuring a source IP pool used for Web server connection

About this task

By default, the device uses the IP address of the outgoing interface in the default route to establish TCP connections with Web servers. An IP address supports a maximum of 65535 TCP connections. To allow the device to establish more TCP connections with Web servers, you can configure source IP pools. The device will use an IP address in the source IP pools for Web server connection.

Restrictions and guidelines

You can specify a maximum of 64 source IP pools. An IP pool can contain a maximum of 512 IP addresses. The IP addresses in different source IP pools cannot overlap with each other.

Procedure

1. Enter system view.

system-view

2. Enter the view of an HTTP proxy service.

Centralized devices:

http-proxy service *service-name*

Distributed devices in standalone mode:Centralized IRF devices:

http-proxy service *service-name* **slot** *slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*

3. Configure a source IP pool used for Web server connection.

ip-pool *start-address end-address* [**vpn-instance** *vpn-instance-name*]

By default, no source IP pools are specified for Web server connection.

Enabling caching of Web server resources

About this task

You can enable this feature to cache Web server resources locally. When a client requests the same Web server resources, the device uses the locally saved data to response the client directly. This method reduces the traffic sent to the servers, reduces the traffic transmission cost, lessens the burden on the servers, reduces the response time of the device to the clients, and enhances the user experience.

Prerequisites

Before configuring the cache file directory for an HTTP proxy service, first disable the HTTP proxy service.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy service.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode:Centralized IRF devices:
http-proxy service *service-name slot slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name chassis chassis-number slot slot-number*
3. Enable the device to cache Web server resources and specify the directory for storing cache files.
cache-data directory *directory*
By default, the device does not cache Web server resources and the directory for storing cache files is not specified.

Specifying a keyword to be monitored and a keyword to replace the monitored keyword

About this task

If the webpage on the Web servers proxied by an HTTP proxy service contains sensitive information, you can configure this feature to specify the keywords to be monitored and to specify the keywords to replace the monitored keywords. To view the monitored keywords and keywords used to replace the monitored keywords, execute the **display http-proxy monitor-info** command. After you specify the keywords to be monitored and the keywords used to replace the monitored keywords for an HTTP proxy service, the HTTP proxy service will use the specified keywords to replace the monitored keywords and send the keywords to the IPv6 clients.

Prerequisites

Before specifying a keyword to be monitored by an HTTP proxy service or specifying the keyword to replace the monitored keyword, first disable the HTTP proxy service.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy service.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode:Centralized IRF devices:
http-proxy service *service-name slot slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name chassis chassis-number slot slot-number*
3. Specify a keyword to be monitored by the HTTP proxy service and a keyword to replace the monitored keyword.

keyword monitor *keyword-string*

By default, no keywords are specified to be monitored by an HTTP proxy service.

Enabling referer protection

About this task

This feature prevents illegal clients from accessing or stealing the webpage resources on the Web servers proxied by an HTTP proxy service. With this feature enabled for an HTTP proxy service, the HTTP proxy service will match the referer field in the HTTP or HTTPS request of a client with the specified allowlist domain names. If no match is found, the device will reject the HTTP or HTTPS requests. Enable this feature when multiple types of resource addresses exist on the webpages of the Web servers proxied by an HTTP proxy service.

Prerequisites

Before enabling referer protection for an HTTP proxy service, first disable the HTTP proxy service.

To make the referer protection feature take effect, first execute the **domain-name** command to specify an allowlist domain name.

Procedure

1. Enter system view.

system-view

2. Enter the view of an HTTP proxy service.

Centralized devices:

http-proxy service *service-name*

Distributed devices in standalone mode: Centralized IRF devices:

http-proxy service *service-name slot slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name chassis chassis-number slot slot-number*

3. Enable referer protection for the HTTP proxy service.

referer-protection enable

By default, the referer protection feature for an HTTP proxy service is disabled.

Enabling URL protection

About this task

This feature can prevent the clients from inserting SQL or XSS statements into the requests to trick the servers into executing malicious SQL or XSS commands, enhancing the security and stability of the network.

Prerequisites

Before enabling URL protection for an HTTP proxy service, first disable the HTTP proxy service.

Procedure

1. Enter system view.

system-view

2. Enter the view of an HTTP proxy service.

Centralized devices:

http-proxy service *service-name*

Distributed devices in standalone mode:Centralized IRF devices:

http-proxy service *service-name* **slot** *slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*

3. Enable URL protection for the HTTP proxy service.

url-protection enable

By default, the URL protection feature for an HTTP proxy service is disabled.

Enabling an HTTP proxy service

1. Enter system view.

system-view

2. Enter the view of an HTTP proxy service.

Centralized devices:

http-proxy service *service-name*

Distributed devices in standalone mode:Centralized IRF devices:

http-proxy service *service-name* **slot** *slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*

3. Enable the HTTP proxy service.

service enable

By default, an HTTP proxy service is disabled.

Configuring the HTTP proxy operation recording

About this task

This feature enables an HTTP proxy service to record all proxy operations in chronological order in a file and save the file in the specified directory. You can execute the **more** command to view the content of the file. For more information about the **more** command, see file management commands in *Fundamentals Command Reference*.

With this feature configured, the device will create a directory named as the main file name of the recording file plus suffix **_history** to store the historical HTTP operation records. For example, if you specify directory **flash:/httpproxy/record.log** to store HTTP operation records, the device automatically creates directory **flash:/httpproxy/record_history** to store historical HTTP operation records. When file **record.log** exceeds the upper limit, the device will create a file named as **record_YYYYMMDDhhmm.log** in directory **flash:/httpproxy/record_history** to store the contents of the **record.log** file and will clear the contents of the **record.log** file. By default, the maximum file size is 10 MB. For the **record_YYYYMMDDhhmm.log** file name, YYYY represents year, MM represents month, DD represents day, hh represents hour, and mm represents minute.

Procedure

1. Enter system view.

system-view

2. Enter the view of an HTTP proxy service.

Centralized devices:

http-proxy service *service-name*

Distributed devices in standalone mode:Centralized IRF devices:

http-proxy service *service-name* **slot** *slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*

3. Enable the HTTP proxy operation recording and specify the directory for saving the HTTP proxy operation recording file.

access-record enable file-path *path* [**gzip**]

By default, the HTTP proxy operation recording is disabled and no directory is specified for saving the HTTP proxy operation recording file.

4. (Optional.) Specify the size of the log file zone and the size of a single log file.

access-record max-size *max-zone-size* **single-file-size** *single-file-size*

By default, the size for a single file is 10 MB and the size of the log file zone is 4 GB.

Display and maintenance commands for HTTP proxy in an HTTP proxy service view

Execute **display** commands in any view.

Task	Command
Display HTTP proxy configuration information in an HTTP proxy service view.	display http-proxy { server-group [<i>group-name</i>] service [<i>service-name</i>] }
Display keyword monitoring information of an HTTP proxy service.	display http-proxy monitor-info service <i>service-name</i> [keyword <i>monitor-string</i>]

Command reference

Modified command: access-record enable

Use **access-record enable** to enable the HTTP proxy operation recording and specify the directory for saving an HTTP proxy operation recording file.

Use **undo access-record enable** to restore the default.

Old syntax

access-record enable file-path *path*

undo access-record enable

New syntax

access-record enable file-path *path* [**gzip**]

undo access-record enable

Views

System view

Change description

The **gzip** keywords is added to the command to compress the HTTP proxy operation recording file. The HTTP proxy operation recording files will be saved in gzip format. If you do not specify this keyword, the device will not compress the HTTP proxy operation recording file.

The following usage guidelines for this command are added:

With this command configured, the device will create a directory named as the main file name of the recording file plus suffix **_history** to store the historical HTTP operation records. For example, if you specify directory **flash:/httpproxy/record.log** to store HTTP operation records, the device automatically creates directory **flash:/httpproxy/record_history** to store historical HTTP operation records. When file **record.log** exceeds the upper limit, the device will create a file named as **record_YYYYMMDDhhmm.log** in directory **flash:/httpproxy/record_history** to store the contents of the **record.log** file and will clear the contents of the **record.log** file. By default, the maximum file size is 10 MB. For the **record_YYYYMMDDhhmm.log** file name, YYYY represents year, MM represents month, DD represents day, hh represents hour, and mm represents minute.

New command: access-record max-size

Use **access-record max-size** to specify the size of the log file zone and the size of a single log file.

Use **undo access-record max-size** to restore the default.

Syntax

access-record max-size *max-zone-size* **single-file-size** *single-file-size*

undo access-record max-size

Default

The size for a single file is 10 MB and the size of the log file zone is 4 GB.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

max-zone-size: Specifies the size of the log file zone. The value range is 500 to 20480 MB.

single-file-size *single-file-size*: Specifies the size of a single log file. The value range for the *single-file-size* argument is 10 to 300 MB.

Usage guidelines

The system automatically saves the proxy information into several HTTP proxy operation files in sequence. If the upper limit of an HTTP proxy operation file is reached, the system creates a new file to save the proxy information. When the upper limit of the log file zone is reached, the early generated proxy information will be overwritten by the newly generated proxy information.

As a best practice, obey the following rules to set the size of a single log file:

- If the device handles a large number of connections, use a smaller value as the size of a single log file. Thus, the device can perform a more granular file overwritten operation when the log file zone is full.
- If the device handles a small number of connections, use a larger value as the size of a single log file to obtain the completed proxy information.

When you specify the size of the log file zone, make sure it is smaller than the maximum size of data that can be stored in the working path.

Examples

(Centralized devices.) Specify 5120 MB and 10 MB as the size of the log file zone and the size of a single log file, respectively.

```
<Sysname> system-view
```

```
[Sysname] http-proxy service test
```

```
[Sysname-http-proxy-service-test]access-record max-size 5120 single-file-size 10
# (Centralized IRF devices.) (Distributed devices in standalone mode.) Specify 5120 MB and 10 MB
as the size of the log file zone and the size of a single log file, respectively.
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] access-record max-size 5120 single-file-size 10
```

Related commands

access-record enable

New command: cache-data

Use **cache-data** to enable the device to cache Web server resources and specify the directory for storing cache files.

Use **undo cache-data** to disable the device from caching Web server resources.

Syntax

cache-data directory *directory*

undo cache-data

Default

The device does not cache Web server resources and the directory for storing cache files is not specified.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

directory *directory*: Specifies a directory path. (Centralized devices.)

directory *directory*: Specifies a directory path. The directory path specified by the *directory* argument must include the slot number in the format of **slotn#** to specify the location of the storage media. The *n* indicates the slot number of the module that has storage media. (Distributed devices in standalone mode.) (Centralized IRF devices.)

directory *directory*: Specifies a directory path. The directory path specified by the *directory* argument must include the chassis number and slot number in the format of **chassism#slotn#** to specify the location of the storage media. The *m* and *n* indicate the member number of the device and the slot number of the module that has storage media, respectively. (Distributed devices in IRF mode.)

Usage guidelines

This command enables the device to cache the Web server resources obtained through the HTTP or HTTPS protocol in the specified directory. When a client requests the same Web server resources, the device uses the locally saved data to response the client directly. This method reduces the traffic sent to the servers, reduces the traffic transmission cost, lessens the burden on the servers, reduces the response time of the device to the clients, and enhances the user experience.

After you execute this command on a centralized IRF device, the distributed devices, or distributed devices in IRF mode, the system will check whether the specified cache files exist on the master device or active MPU:

- If yes, the configuration succeeds.

- If not, the configuration fails.

Before changing the cache file directory for an HTTP proxy service, make sure the HTTP proxy service is disabled.

If you execute this command multiple times, the most recent configuration takes effect.

Currently, the device can cache the apk, bmp, doc, docx, gif, gzip, ipa, jar, jpg, jpeg, mp4, pdf, png, pptx, rar, swf, tar, txt, xls, xlsx, or zip files on the webpages.

Examples

(Centralized devices.) Enable HTTP proxy service **test** to cache Web server resources and specify directory **flash:/cached** to store cache files.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] cache-data directory flash:/cached
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Enable HTTP proxy service **test** to cache Web server resources and specify directory **flash:/cached** to store cache files.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] cache-data directory slot1#flash:/cached
```

Related commands

service enable

New command: denylist-domain-name

Use **denylist-domain-name** to specify a denylist domain name for an HTTP proxy service.

Use **undo denylist-domain-name** to delete a denylist domain name for an HTTP proxy service.

Syntax

denylist-domain-name *domain-name*

undo denylist-domain-name *domain-name*

Default

No denylist domain names are specified for an HTTP proxy service.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a denylist domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

When a client accesses a website through an HTTP proxy service, the device returns an error page to the client if the domain name of the requested website is in the domain name denylist. When a client accesses an external link on the website proxied by an HTTP proxy service, the device returns an error page to the client if the domain name of the requested external link is in the domain name denylist.

An external link is a hyperlink that exists on the webpages of an IPv4 server accessed by a client and is used to redirect to other websites.

If you do not specify a denylist domain name or allowlist domain name for an HTTP proxy service, the device can proxy all domain names. If you specify only denylist domain names for an HTTP proxy service, the device can proxy all domain names except the domain names in the denylist. If you specify only allowlist domain names for an HTTP proxy service, the device can only proxy the domain names in the allowlist.

A maximum of 512 denylist domain names can be configured. You can execute this command multiple times to configure multiple denylist domain names.

A domain name can only be added to the domain name allowlist or the domain name denylist. The **denylist-domain-name** and **domain-name** commands are mutually exclusive.

Before specifying a denylist domain name for an HTTP proxy service, first disable the HTTP proxy service.

Examples

(Centralized devices.) Add domain name **test.gov.cn** to the domain name denylist for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] denylist-domain-name test.gov.cn
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Add domain name **test.gov.cn** to the domain name denylist for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] denylist-domain-name test.gov.cn
```

Related commands

domain-name

service enable

Modified command: display http-proxy

Use **display http-proxy** to display HTTP proxy configuration information.

Syntax

```
display http-proxy { server-group [ group-name ] | service [ service-name ] }
```

Views

Any view

Change description

The displayed configuration information about an HTTP proxy service has changed.

Display the configuration information about HTTP proxy service **test**.

```
<Sysname> display http-proxy service test
Service name: test
  IPv6 address:                2001::1
  Allowlist domain names:      www.aaa.com
                               www.bbb.com
                               www.ccc.com
  Protocol types:              HTTP at port 8000
                               HTTP   [Server group: testa]
```

```

HTTP at port 8001 [Server group: testa]
HTTPS at port 8003
HTTPS [Server group: testb]
HTTPS at port 8002 [Server group: testb]
SSL certificate directory: flash:/
Domain name: www.aaa.com
  SSL certificate file: aaa.cert
  SSL key files: aaa.key
Domain name: www.bbb.com
  SSL certificate file: bbb.cert
  SSL key files: bbb.key
Hyperlink proxy strings: www.hyperlink.org
                        www.org.com
DNS servers: 8.8.8.8
             9.9.9.9
Denylist domain names: www.fff.com
                       www.eee.com
Monitored keyword: abc
  Replaced by: efg
Monitored keyword: def
  Replaced by: N/A
Excluded external domain name: www.abc.com
IP pools: 1.1.1.1 to 1.1.1.2 vpn1
          2.2.2.1 to 2.2.3.1 vpn1
Wildcard domain name: extlink.cn
URL protection: Enabled
Referer protection: Enabled
Extlink href: Enabled
Medialink proxy: Enabled
Cache data: Enabled
  Cache file path: flash:/httpproxy
HTTP proxy operation recording: Enabled
  Operation record file path: flash:/httpproxy/20210111.log gzip
  Max zone size: 4096MB
  Single file size: 10MB
HTTP proxy status: Enabled

```

Table 79 Command output

Field	Description
HTTP proxy name	HTTP proxy service name.
IPv6 address	IPv6 address specified for the HTTP proxy service, which can be resolved from the specified domain name. This field displays N/A if no IPv6 address is specified for the HTTP proxy service.
Allowlist domain names	Allowlist domain names for the HTTP proxy service, which can be resolved to the specified IPv6 address. This field displays N/A if no allowlist domain name is specified for the HTTP proxy service.

Field	Description
Domain name	Domain name specified for the HTTP proxy service. The domain name corresponds to the specified IPv6 address. This field displays N/A if no domain name is specified for the HTTP proxy service.
Protocol types	Protocol types specified for the HTTP proxy service, listening port number, and the Web server groups bound to the HTTP proxy service. This field displays N/A if no protocol types are specified for the HTTP proxy service.
SSL certificate file	SSL certificate file specified for the HTTP proxy service. This field displays N/A if no SSL certificate file is specified for the HTTP proxy service.
SSL certificate key-file	SSL certificate key file specified for the HTTP proxy service. This field displays N/A if no SSL certificate key file is specified for the HTTP proxy service.
SSL certificate directory	Directory of SSL certification files and SSL certificate key files. This field displays N/A if the directory of the SSL certification files and SSL certificate key files is not specified.
Domain name	Domain name specified for the HTTPS requests of the HTTP proxy service. This field displays N/A if no domain name is specified for the HTTPS requests of the HTTP proxy service.
SSL key file	SSL certificate key file specified for the HTTP proxy service. This field displays N/A if no SSL certificate key file is specified for the HTTP proxy service.
Hyperlink proxy strings	External hyperlink match strings specified for the HTTP proxy service. This field displays N/A if no external hyperlink strings are specified for the HTTP proxy service.
DNS servers	IP addresses of the DNS servers. This field displays N/A if no DNS server is specified.
Denylist domain names	Denylist domain names for the HTTP proxy service. This field displays N/A if no denylist domain name is specified for the HTTP proxy service.
Monitored keyword	Monitored keyword of the HTTP proxy service. This field displays N/A if no keyword is specified to be monitored by the HTTP proxy service.
Replaced by	Keyword to replace the monitored keyword. This field displays N/A if no keyword is specified to replace the monitored keyword of the HTTP proxy service.
Excluded external domain name	Domain name of the external link that will not be proxied by the HTTP proxy service. This field displays N/A if you have not specified the external link domain name to be not proxied by the HTTP proxy service.
IP pools	Source IP pools used for Web server connection. This field displays N/A if no IP pool is specified for the HTTP proxy.
Wildcard domain name	Wildcard domain name for the HTTP proxy service. This field displays N/A if no wildcard domain name is specified for the HTTP proxy service.

Field	Description
URL protection	URL protection status of the HTTP proxy service: • Enabled. • Disabled.
Referer protection	Referer protection status of the HTTP proxy service: • Enabled. • Disabled.
Extlink href	External link reference status of the HTTP proxy service: • Enabled. • Disabled.
Medialink proxy	Status of the external media link proxy feature: • Enabled. • Disabled.
Cache data	Web resource caching status of the HTTP proxy service: • Enabled. • Disabled.
Cache file path	Path for saving the cache files of the HTTP proxy service. This field displays N/A if no cache file path is specified.
HTTP proxy operation recording	Status of the HTTP proxy operation recording feature: • Enabled. • Disabled.
Operation record file path	Directory for saving an HTTP proxy operation recording file. This field displays N/A if no directory is specified for saving an HTTP proxy operation recording file. If an HTTP proxy operation recording file is compressed, this field displays the directory and file compression format.
Max zone size	Maximum size of the log file zone. This field displays N/A if no maximum size is specified for the log file zone.
Single file size	Size of a single file. This field displays N/A if no size is specified for a single log file.
HTTP proxy status	Status of the HTTP proxy service: • Enabled. • Disabled.

New command: display http-proxy monitor-info

Use **display http-proxy monitor-info** to display keyword monitoring information of an HTTP proxy service.

Syntax

display http-proxy monitor-info service *service-name* [**keyword** *monitor-string*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service *service-name*: Specifies an HTTP proxy service by its name, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_).

keyword *monitor-string*: Specifies a monitored keyword. The *monitor-string* argument is a string of 1 to 127 characters and supports Chinese characters in UTF-8 encoding format. If you do not specify this option, this command displays information about all monitored keyword.

Examples

Display information about monitored and replaced keywords by HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname]display http-proxy monitor-info service test
  Monitored keyword:      aabbcc
  Time:                   2021/01/11 20:39:38
  URL:                    http://a.com/index.html
  Replaced by:            bddcc

  Monitored keyword:      qqwwee
  Time:                   2021/01/11 20:39:38
  URL:                    http://b.com/index.html
  Replaced by:            N/A
```

Table 80 Command output

Field	Description
Monitored keyword	Keyword monitored by the HTTP proxy service.
Time	Time when the device finds the monitored keyword.
URL	URL of the monitored keyword.
Replaced by	Keyword used to replace the monitored keyword. This field displays N/A if no keyword is specified to replace the monitored keyword.

Modified command: dns-server

Use **dns-server** to specify a DNS server for an HTTP proxy service.

Use **undo dns-server** to remove a DNS server for an HTTP proxy service.

Syntax

dns-server *ip-address*

undo dns-server *ip-address*

Views

HTTP proxy service view

Change description

The usage guidelines for this command have changed.

- Before modification:

Configure a minimum of one DNS server for an HTTP proxy service to resolve the domain names of the external hyperlinks and media links to be proxied on webpages of the Web servers.

- After modification:

This command configures a DNS server to resolve the domain names of the Web servers. To enable the device to proxy hyperlinks on the Web servers or to proxy Web servers using different domain names, configure a minimum of one DNS server for an HTTP proxy service.

Modified command: domain-name

Use **domain-name** to specify an allowlist domain name for an HTTP proxy service.

Use **undo domain-name** to delete an allowlist domain name for an HTTP proxy service.

Old syntax

domain-name *domain-name*

undo domain-name

New syntax

domain-name *domain-name*

undo domain-name *domain-name*

Views

HTTP proxy service view

Change description

The function of this command has changed:

- Before modification:

Use **domain-name** to specify a domain name for an HTTP proxy service.

Use **undo domain-name** to delete the domain name for an HTTP proxy service.

- After modification:

Use **domain-name** to specify an allowlist domain name for an HTTP proxy service.

Use **undo domain-name** to delete an allowlist domain name for an HTTP proxy service.

The following usage guidelines for the **domain-name** command are added:

After you configure allowlist domain names, when a client tries to access a website through the proxy service, the device returns an error page to the client if the domain name of the requested website is not in the allowlist.

If you have not configured the wildcard domain name or enabled external link reference for an HTTP proxy service, the device responds a new domain name to a client who requests to access an external link on a Web server. The new domain name is composed of the domain name specified by this command plus the domain name of the external link. Thus, the device can use the specified DNS server to resolve new domain name into the IP address of the server that stores the external link resource. For a client, the domain name specified by this command must be the same as the domain name of the Web server accessed by the client.

For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.

A maximum of 512 allowlist domain names can be configured in a view. You can execute this command multiple times to configure multiple allowlist domain names.

A domain name can only be added to the domain name allowlist or the domain name denylist. The **denylist-domain-name** and **domain-name** commands are mutually exclusive.

Before specifying an allowlist domain name for an HTTP proxy service, first disable the HTTP proxy service.

New command: **exclude-external-domain**

Use **exclude-external-domain** to specify an external link domain name not to be proxied by an HTTP proxy service, hereinafter referred to as excluded external domain name.

Use **undo exclude-external-domain** to remove an excluded external domain name.

Syntax

exclude-external-domain *domain-name*

undo exclude-external-domain *domain-name*

Default

No excluded external domain names are specified for an HTTP proxy service.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an external link domain name, a case-insensitive string of 1 to 253 characters. Valid characters in the domain name string include letters, digits, hyphens (-), and underscores (_).

Usage guidelines

After you configure this command, the device will not add the domain name of an HTTP proxy service to the specified external link domain name. Thus, the clients cannot access the external link of the specified domain name through the HTTP proxy service. Please use this feature with cautions. For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.

Before specifying an excluded external domain name for an HTTP proxy service, disable the HTTP proxy service.

A maximum of 512 external link domain names can be configured. You can execute this command multiple times to configure multiple external link domain names.

A domain name can only be proxied or not proxied. The **exclude-external-domain** and **hyperlink-proxy** commands are mutually exclusive.

Examples

(Centralized devices.) Configure HTTP proxy service **test** to not proxy the requests for external links of domain name **test.gov.cn**.

```
<Sysname> system-view
```

```
[Sysname] http-proxy service test
```

```
[Sysname-http-proxy-service-test] exclude-external-domain test.gov.cn
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Configure HTTP proxy service **test** to not proxy the requests for external links of domain name **test.gov.cn**.

```
<Sysname> system-view
```

```
[Sysname] http-proxy service test slot 1
```

```
[Sysname-http-proxy-service-test-slot1] exclude-external-domain test.gov.cn
```

Related commands

service enable

hyperlink-proxy

New command: extlink-href enable

Use **extlink-href enable** to enable external link reference for an HTTP proxy service.

Use **undo extlink-href enable** to disable external link reference for an HTTP proxy service.

Syntax

extlink-href enable

undo extlink-href enable

Default

The external link reference feature for an HTTP proxy service is disabled.

Views

HTTP proxy service view

Predefined user roles

network-admin

Usage guidelines

The external link reference feature enables the clients to access all external links on webpages of any Web server. To configure the device to not proxy the requests for external links of a specific domain name, execute the **exclude-external-domain** command. For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.

To use this feature, you must execute the **wildcard-domain-name** command. After you configure a wildcard domain name and enable the external link reference feature, the device will add the specified wildcard domain name to the external link domain name that is requested by a client.

Before enabling external link reference for an HTTP proxy service, first disable the HTTP proxy service.

Examples

(Centralized devices.) Enable external link reference for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] extlink-href enable
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Enable external link reference for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] extlink-href enable
```

Related commands

wildcard-domain-name

service enable

exclude-external-domain

Modified command: hyperlink-proxy

Use **hyperlink-proxy** to specify an external link to be proxied by an HTTP proxy service.

Use **undo hyperlink-proxy** to remove an external link from the external hyperlinks proxied by an HTTP proxy service.

Syntax

hyperlink-proxy *link-string*

undo hyperlink-proxy *link-string*

Views

HTTP proxy service view

Change description

The function of this command has changed:

- Before modification:
 - Use **hyperlink-proxy** to specify an external hyperlink to be proxied on webpages.
 - Use **undo hyperlink-proxy** to remove an external hyperlink to be proxied on webpages.
- After modification:
 - Use **hyperlink-proxy** to specify an external link to be proxied by an HTTP proxy service.
 - Use **undo hyperlink-proxy** to remove an external link from the external hyperlinks proxied by an HTTP proxy service.

The default for this command has changed:

- Before modification:
 - No external hyperlinks to be proxied are specified on webpages.
- After modification:
 - No external links to be proxied are specified for an HTTP proxy service.

The usage guidelines for this command have changed:

- Before modification:
 - This feature enables users to access external hyperlinks on webpages of Web servers proxied by the HTTP proxy service.
 - Execute this command when the HTTP proxy service is disabled.
- After modification:
 - By default, the clients cannot use an HTTP proxy service to access external links. In HTTP proxy service view, you can specify external links to be proxied by the HTTP proxy service. For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.
 - Before specifying an external link to be proxied by an HTTP proxy service, first disable the HTTP proxy service.

New command: keyword monitor

Use **keyword monitor** to specify a keyword to be monitored by an HTTP proxy service and a keyword to replace the monitored keyword.

Use **undo keyword** to cancel the monitoring on a keyword.

Syntax

keyword monitor *keyword-string*

undo keyword monitor *monitor-string*

Default

No keywords are specified to be monitored by an HTTP proxy service.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

keyword-string: Specifies a keyword to be monitored and a keyword to replace the monitored keyword. The *keyword-string* argument is a string of 1 to 255 characters and supports Chinese characters in UTF-8 encoding format. If you specify both a monitored keyword and a keyword to replace the monitored keyword, make sure the keywords are specified in sequence and separated by spaces. For example, the string **abc def** represents that keyword **def** is specified to replace monitored keyword **abc**. If you do not need to specify a keyword to replace the monitored keyword, just enter a monitored keyword.

Usage guidelines

To specify multiple keywords to be monitored by an HTTP proxy service, execute this command multiple times. A maximum of 512 keywords can be monitored by an HTTP proxy service.

You can execute this command to specify the keywords to be monitored by the device and to specify the keywords to replace the monitored keywords. To view the monitored keywords and keywords used to replace the monitored keywords, execute the **display http-proxy** or **display http-proxy monitor-info** command.

Before modifying the keyword monitored by an HTTP proxy service or modifying the keyword used to replace the monitored keyword, first disable the HTTP proxy service.

Examples

Configure HTTP proxy service **test** to monitor keyword **abc**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] keyword monitor abc
```

Configure HTTP proxy service **test** to monitor keyword **abc** and to use keyword **def** to replace monitored keyword **abc**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] keyword monitor abc def
```

Related commands

service enable

display http-proxy monitor-info

Modified command: medialink-proxy enable

Use **medialink-proxy enable** to enable the external media link proxy feature for an HTTP proxy service.

Use **undo medialink-proxy enable** to disable the external media link proxy feature for an HTTP proxy service.

Syntax

medialink-proxy enable

undo medialink-proxy enable

Views

HTTP proxy service view

Change description

The function of this command has changed:

- Before modification:
 - Use **medialink-proxy enable** to enable the external media link proxy feature.
 - Use **undo medialink-proxy enable** to disable the external media link proxy feature.
- After modification:
 - Use **medialink-proxy enable** to enable the external media link proxy feature for an HTTP proxy service.
 - Use **undo medialink-proxy enable** to disable the external media link proxy feature for an HTTP proxy service.

The default for this command has changed:

- Before modification:
 - The external media link proxy feature is disabled.
- After modification:
 - The external media link proxy feature for an HTTP proxy service is disabled.

New command: referer-protection enable

Use **referer-protection enable** to enable referer protection for an HTTP proxy service.

Use **undo referer-protection enable** to disable referer protection for an HTTP proxy service.

Syntax

referer-protection enable

undo referer-protection enable

Default

The referer protection feature for an HTTP proxy service is disabled.

Views

HTTP proxy service view

Predefined user roles

network-admin

Usage guidelines

With the referer protection feature enabled for an HTTP proxy service, the HTTP proxy service will match the referer field in the HTTP request of a client with the specified allowlist domain names. Thus the HTTP proxy service can filter the HTTP request for website resources and prevent other websites from stealing webpage resources of the proxied Web servers. To make the referer protection feature take effect, first execute the **domain-name** command to specify the allowlist domain names.

Before enabling referer protection for an HTTP proxy service, first disable the HTTP proxy service.

Examples

(Centralized devices.) Enable referer protection for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] referer-protection enable
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Enable referer protection for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] referer-protection enable
```

Related commands

domain-name

service enable

New command: ssl certificate directory

Use **ssl certificate directory** to specify a directory to store SSL certificates and SSL certificate key files.

Use **undo ssl certificate directory** to cancel the directory configuration.

Syntax

ssl certificate directory *directory*

undo ssl certificate directory

Default

No directory is specified to store SSL certificates and SSL certificate key files.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory to store SSL certificate files and SSL certificate key files. (Centralized devices.)

directory: Specifies a directory to store SSL certificate files and SSL certificate key files. The directory specified by the *directory* argument must include the slot number in the format of **slotn#** to specify the location of the storage media. The *n* indicates the slot number of the active MPU or master device that has storage media. (Distributed devices in standalone mode.) (Centralized IRF devices.)

directory: Specifies a directory to store SSL certificate files and SSL certificate key files. The directory specified by the *directory* argument must include the chassis number and slot number in the format of **chassis#slotn#** to specify the location of the storage media. The *m* and *n* indicate the member number of the master device and the slot number of the active MPU that has storage media, respectively. (Distributed devices in IRF mode.)

Usage guidelines

For an HTTP proxy service to proxy HTTPS requests, you must specify an SSL certificate file and SSL certificate key file for the HTTP proxy service. This command specifies the directory to store SSL certificate files and SSL certificate key files.

After you execute this command, the system will check whether the specified directory exists:

- If yes, the configuration succeeds.
- If not, the configuration fails.

Before modifying the directory for storing SSL certificate files and SSL certificate key files for an HTTP proxy service, first disable the HTTP proxy service.

If you execute this command multiple times, the most recent configuration takes effect. The directory specified by this command is used to store SSL certificate files and SSL certificate key files specified by the **ssl certificate domain-name file key-file** command.

This command is mutually exclusive with the **ssl certificate file** command and the **ssl certificate key-file** command.

Examples

(Centralized devices.) Specify directory **flash:/ssl-certificate** for HTTP proxy service **test** to store SSL certificate files and SSL certificate key files.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] ssl certificate directory flash:/ssl-certificate
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Specify directory **slot1#flash:/ssl-certificate** for HTTP proxy service **test** to store SSL certificate files and SSL certificate key files.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] ssl certificate directory
slot1#flash:/ssl-certificate
```

Related commands

protocol-type (HTTP proxy service view)

ssl certificate domain-name file key-file

service enable

New command: ssl certificate domain-name file key-file

Use **ssl certificate domain-name file key-file** to specify an SSL certificate file and SSL certificate key file for an HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.

Use **undo ssl certificate domain-name** to delete the specified SSL certificate file and SSL certificate key file for an HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.

Syntax

ssl certificate domain-name *domain-name* **file** *certificate-file* **key-file** *key-file*

undo ssl certificate [**domain-name** *domain-name*]

Default

No SSL certificate file and SSL certificate key file are specified for an HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).

certificate-file: Specifies an SSL certificate file.

key-file: Specifies an SSL certificate key file.

Usage guidelines

For an HTTP proxy service to proxy HTTPS requests for a specific domain name, you must specify an SSL certificate file and SSL certificate key file for the HTTP proxy service. The SSL certificate files and SSL certificate key files are stored in the directory specified by the **ssl certificate directory** command.

Before executing this command, make sure the specified SSL certificate file and SSL certificate key file already exist in the directory. Otherwise, the configuration fails.

To allow an HTTP proxy service to proxy the HTTPS requests for the specified domain name, first specify an SSL certificate file and SSL certificate key file and then enable the HTTP proxy service.

Before modifying the SSL certificate file and SSL certificate key file for an HTTP proxy service, first disable the HTTP proxy service.

To allow an HTTP proxy service to proxy HTTPS requests for one domain name, you can execute this command multiple times but only the most recent configuration takes effect. To allow an HTTP proxy service to proxy HTTP requests for multiple domain names, you can execute this command multiple times. An HTTP proxy service supports a maximum of 128 pairs of SSL certificate files and SSL certificate key files.

This command is mutually exclusive with the **ssl certificate file** command and the **ssl certificate key-file** command.

Examples

Specify SSL certificate file **cert.pem** and SSL certificate key file **cert.key** for HTTP proxy service **test** to allow it to proxy the HTTPS requests for domain name **test.gov.cn**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] ssl certificate domain-name test.gov.cn file cert.pem
key-file cert.key
```

Related commands

protocol-type (HTTP proxy service view)

ssl certificate directory

service enable

New command: url-protection enable

Use **url-protection enable** to enable URL protection for an HTTP proxy service.

Use **undo url-protection enable** to disable URL protection for an HTTP proxy service.

Syntax

url-protection enable

undo url-protection enable

Default

The URL protection feature for an HTTP proxy service is disabled.

Views

HTTP proxy service view

Predefined user roles

network-admin

Usage guidelines

The URL protection feature can prevent the clients from inserting SQL or XSS statements into the requests to trick the servers into executing malicious SQL or XSS commands. If the device needs to proxy the requests to the websites containing databases, enable this feature as a best practice.

Before enabling URL protection for an HTTP proxy service, first disable the HTTP proxy service.

Examples

(Centralized devices.) Enable URL protection for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] url-protection enable
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Enable URL protection for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] url-protection enable
```

Related commands

service enable

New command: wildcard-domain-name

Use **wildcard-domain-name** to specify the wildcard domain name for an HTTP proxy service.

Use **undo wildcard-domain-name** to restore the default.

Syntax

wildcard-domain-name *wildcard-domain-name*

undo wildcard-domain-name

Default

No wildcard domain name is specified for an HTTP proxy service.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

wildcard-domain-name: Specifies a wildcard domain name, a case-insensitive string of 1 to 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for

example). Each domain name suffix can contain a maximum of 63 characters. Valid characters in the domain name string include letters, digits, hyphens (-), and underscores (_).

Usage guidelines

To allow an HTTP proxy service to proxy the requests for different external links of different domain names, you can specify a wildcard domain name for the HTTP proxy service and enable the external link reference feature. Otherwise, you need to execute the **domain-name** command multiple times to allow an HTTP proxy service to proxy the requests for different external links of the different domain names. For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.

When a client accesses an external link, the device adds the specified wildcard domain name to the external link domain name and returns the new domain name to the client. After the device receives the HTTP or HTTPS requests containing the wildcard domain name, it strips the wildcard domain name and sends the external link domain name to a DNS server to resolve the IP address. The DNS server returns the resolved IP address to the device, thus the device can proxy the requests to the external link.

Before specifying the wildcard domain name for an HTTP proxy service, disable the HTTP proxy service.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

(Centralized devices.) Specify wildcard domain name **abc.cn** for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] wildcard-domain-name abc.cn
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Specify wildcard domain name **abc.cn** for HTTP proxy service **test**.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] wildcard-domain-name abc.cn
```

Related commands

extlink-href enable

service enable

dns-server

New command: display system internal http-proxy service fail

Use **display system internal http-proxy service fail** to display information about HTTP proxy failures between the device and Web servers.

Syntax

Centralized devices:

display system internal http-proxy service *service-name* fail

Distributed devices in standalone mode: Centralized IRF devices:

display system internal http-proxy service *service-name* fail slot *slot-number*

Distributed devices in IRF mode:

display system internal http-proxy service *service-name* fail chassis *chassis-number* slot *slot-number*

Views

Probe view

Predefined user roles

network-admin

network-operator

Parameters

service-name: Specifies an HTTP proxy service by its name, a case-insensitive string of 1 to 63 characters. Valid characters include digits, letters, and underscores (_).

slot *slot-number*: Specifies a card by its slot number. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. (Centralized IRF devices.) (IRF 3 incapable.)

slot *slot-number*: Specifies an IRF member device by its member ID or specifies a PEX by its virtual slot number. (Centralized IRF devices.) (IRF 3 capable.)

chassis *chassis-number* slot *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (Distributed devices in IRF mode.) (IRF 3 incapable.)

chassis *chassis-number* slot *slot-number*: Specifies a card on an IRF member device or specifies a PEX. The *chassis-number* argument represents the member ID of the IRF member device or the virtual chassis number of the PEX. The *slot-number* argument represents the slot number of the card or PEX. (Distributed devices in IRF mode.) (IRF 3 capable.)

New feature: Configuring HTTP proxy in an HTTP proxy server view

Configuring HTTP proxy in an HTTP proxy server view

Restrictions and guidelines: HTTP proxy in an HTTP proxy server view

To enable an HTTP proxy service to proxy the Web resources, make sure the ports on the device used for communication with the IPv6 user and IPv4 Web server belong to the same slot.

When configuring proxy-related features in an HTTP proxy server view, make sure the current HTTP proxy server view is not referenced. After all proxy configurations are completed, reference the current view and start the HTTP proxy service.

HTTP proxy tasks at a glance

To configure HTTP proxy in an HTTP proxy server view, perform the following tasks:

1. [Creating an HTTP proxy server view](#)
2. [Configuring proxy-related parameters in an HTTP proxy server view](#)

3. [Specifying an SSL certificate file and SSL certificate key file](#)
This task is required only when you configure the device to proxy HTTPS requests. It does not take effect in proxy of HTTP requests.
4. (Optional.) [Configuring the external link proxy feature](#)
5. (Optional.) [Configuring the advanced features in an HTTP proxy server view](#)
 - [Configuring a source IP pool used for Web server connection](#)
 - [Enabling caching of Web server resources](#)
 - [Specifying a keyword to be monitored and a keyword to replace the monitored keyword](#)
 - [Enable referer protection](#)
 - [Enabling URL protection](#)
 - [Deleting response header set-cookie attributes](#)
 - [Enabling the restoration of QueryString in Web requests](#)
 - [Replacing an HTTP or HTTPS response header or restoring an HTTP or HTTPS request header](#)
 - [Configuring a redirect URL domain name that allows replacement](#)
6. [Referencing an HTTP proxy server view](#)
7. (Optional.) [Enabling wildcard domain name encryption feature for an HTTP proxy service](#)
8. (Optional.) [Configuring the HTTP proxy operation recording](#)
9. [Enabling an HTTP proxy service](#)

Creating an HTTP proxy server view

Restrictions and guidelines

You can create multiple HTTP proxy server views on a device to proxy different Web server resources with different parameters. The configurations in an HTTP proxy server view take effect after the view is referenced.

Procedure

1. Enter system view.
system-view
2. Create an HTTP proxy server and enter its view.
http-proxy server *server-name*
By default, no HTTP proxy server view exists.

Configuring proxy-related parameters in an HTTP proxy server view

About this task

An HTTP proxy service listens for and proxies HTTP or HTTPS requests from a specified TCP port number and IPv6 address. To proxy HTTPS packets, you must also specify an SSL certificate file and SSL certificate key file so the device can establish secure connections to IPv6 clients.

After you execute the **domain name** command, the web servers of the domain names specified by the command is the Web resource proxy scope of the device. The device uses the configurations in the HTTP proxy server view to proxy.

Restrictions and guidelines

An HTTP proxy server view supports a maximum of 512 allowlist domain names.

The configurations related to proxy parameters can only be performed in HTTP proxy server view.

Prerequisites

You must specify an unused TCP port number for an HTTP proxy service. To view TCP port numbers in use, execute the **display tcp** command.

For more information about specifying a DNS server for the HTTP proxy service in HTTP proxy service view, see "[Configuring an HTTP proxy service.](#)"

Procedure

1. Enter system view.
system-view
2. Create an HTTP proxy server and enter its view.
http-proxy server *server-name*
3. Specify a protocol type and listening port for the HTTP proxy service.
protocol-type { **http** | **https** } [**port** *port-number*]
By default, no protocol type or listening port number is specified for an HTTP proxy service.
4. Specify an IPv6 address for the HTTP proxy service.
ipv6-address *ipv6-address*
By default, no IPv6 address is specified for an HTTP proxy service.
5. Specify an allowlist domain name for the HTTP proxy service.
domain-name *domain-name*
By default, no allowlist domain names are specified for an HTTP proxy service.

Specifying an SSL certificate file and SSL certificate key file

In proxy of HTTPS requests, you can reuse the configurations in an HTTP proxy service view to configure the feature in HTTP proxy server view. For more information, see "[Specifying an SSL certificate file and SSL certificate key file](#)" in an HTTP proxy service view.

Configuring the external link proxy feature

About configuring the external link proxy feature

For an HTTP proxy server, configure the external link proxy feature as required:

- The external link reference feature enables the HTTP proxy server to proxy all external links on webpages of proxied Web servers by adding the wildcard domain name to the link URLs. In this way, the clients can access the external links of all proxied Web servers. To configure the device to not proxy the requests for external links of a specific domain name, execute the **exclude-external-domain** command.
- The external hyperlink proxy feature enables the HTTP proxy server to add the specified wildcard domain name for all external links on the Web servers with specified domain names. In this way, the clients can access these external links.

When an IPv6 user fails to access the Web page or to request part of the Web resources through an HTTP proxy service, you can take the following actions.

- Enable the external link proxying failure informing feature. If you enable this feature, message **Error on page. Please visit URL XXX.** will display when the external link proxying failure occurs.
- Enable the external link proxying failure redirection feature. This feature redirects the failed external links with the specified error code and allows the IPv6 user to directly access the external link server without using the HTTP proxy service.

Restrictions and guidelines

In configuration of the external link proxy feature, the commands except the **exclude-external-domain** command can only be configured in the HTTP proxy server view.

The external media link proxy feature and the external hyperlink proxy feature configured in HTTP proxy service view do not take effect in HTTP proxy server view.

Prerequisites

To make this feature take effect for an HTTP proxy service, you must specify a wildcard domain name for the HTTP proxy service. For more information, see "[Configuring the external link reference feature](#)" in an HTTP proxy service view.

Configuring the external link reference feature

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Enable external link reference for the HTTP proxy service.
extlink-href enable
By default, the external link reference feature for an HTTP proxy service is disabled.
4. (Optional.) Specify an external link domain name to be not proxied by the HTTP proxy service.
exclude-external-domain *domain-name*
By default, no external link domain names to be not proxied are specified for an HTTP proxy service.
5. (Optional.) Enable the external link proxying failure informing feature.
failed-extlink inform
By default, the external link proxying failure informing feature is disabled.
6. (Optional.) Enable the external link proxying failure redirection feature.
failed-extlink redirect *error-code*
By default, the external link proxying failure redirection feature is disabled.

Configuring the external hyperlink proxy feature

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Specify an external link domain name in an HTTP proxy server view.
include-external-domain *domain-name*

- By default, no external link domain name is configured in an HTTP proxy server view.
4. (Optional.) Enable the external link proxying failure informing feature.
failed-extlink inform
By default, the external link proxying failure informing feature is disabled.
 5. (Optional.) Enable the external link proxying failure redirection feature.
failed-extlink redirect *error-code*
By default, the external link proxying failure redirection feature is disabled.

Configuring the advanced features in an HTTP proxy server view

Configuring a source IP pool used for Web server connection

You can reuse the configurations in an HTTP proxy service view to configure the feature in an HTTP proxy server view. For more information, see "[Configuring a source IP pool used for Web server connection](#)" in an HTTP proxy service view.

Enabling caching of Web server resources

About this task

You can enable this feature to cache Web server resources locally. When a client requests the same Web server resources, the device uses the locally saved data to response the client directly. This method reduces the traffic sent to the servers, reduces the traffic transmission cost, lessens the burden on the servers, reduces the response time of the device to the clients, and enhances the user experience.

Restrictions and guidelines

In reference to an HTTP proxy server view, if the **cache data** command is configured in the view, the directory path specified by the command can only be the path of the slot where the HTTP proxy service view referencing the HTTP proxy server view is located. Otherwise, the reference fails.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Enable the device to cache Web server resources and specify the directory for storing cache files.
cache-data directory *directory*
By default, the device does not cache Web server resources and the directory for storing cache files is not specified.

Specifying a keyword to be monitored and a keyword to replace the monitored keyword

You can reuse the configurations in an HTTP proxy service view to configure the feature in an HTTP proxy server view. For more information, see "[Specifying a keyword to be monitored and a keyword to replace the monitored keyword](#)" in an HTTP proxy service view.

Enable referer protection

About this task

This feature prevents illegal clients from accessing or stealing the webpage resources on the Web servers proxied by an HTTP proxy service. With this feature enabled for an HTTP proxy service in an HTTP proxy server view, the HTTP proxy service will match the referer field in the HTTP or HTTPS request of a client with the specified allowlist domain names. If no match is found, the device will reject the HTTP or HTTPS requests. Enable this feature when multiple types of resource addresses exist on the webpages of the Web servers proxied by an HTTP proxy service.

Prerequisites

If you enable referer protection in both HTTP proxy server view and HTTP proxy service view, the referer field in the HTTP or HTTPS requests sent by the client should meet the feature requirements in both views. Otherwise, the requests will be denied.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Configure a referer allowlist domain name.
referer-protection domain *domain-name* allowlist *allowlist-domain-name*

By default, the referer protection feature for an HTTP proxy service is disabled.

When a client access a domain name, if the domain name in the referer field of the sent HTTP or HTTPS requests is not contained in the allowlist domain names, the device will deny the requests.

Enabling URL protection

You can reuse the configurations in an HTTP proxy service view to configure the feature in an HTTP proxy server view. For more information, see "[Enabling URL protection](#)" in an HTTP proxy service view.

Deleting response header set-cookie attributes

About this task

This feature can be applied in the following situations:

- After the external link reference feature is enabled in an HTTP proxy server view, the device will add a specified wildcard domain name to the external link URL in the response returned by the Web server. Thus, the external link URL is modified into HTTP format. For example, the device modifies external link URL **https://abc.com** into **http://https-abc-com.gov6.cn** by adding wildcard domain name **gov6.cn**. A client sends HTTP requests containing the wildcard domain name to the device when it accesses the external link. After the device receives the HTTP requests containing the wildcard domain name, it strips the

wildcard domain name and restores the external link URL to **https://abc.com**. Then it sends the requests to the Web server through HTTPS protocol.

In the above process, when the Web server returns HTTPS response packets, the response header set-cookie attributes might contain the secure flag. The secure flag can only be used in HTTPS protocol. It ensures a secure transmission (through HTTPS instead of HTTP) of a cookie, thus improving the security of the cookie. Because the client requests external link resources through HTTP, it does not save the cookie when it receives set-cookie attributes containing the secure flag. As a result, the user will go offline when it accesses the external link resources. If you use the delete cookie-flag secure command to delete the secure flag in the set-cookie attributes of the response header returned by the Web server, the client will save the cookie.

- For Web servers with high security, the set-cookie attributes of the HTTP or HTTPS response header returned by the Web server might contain the samesite flag. The samesite flag is used to restrict third-party cookies and prevents illegal websites from forging HTTP or HTTPS requests by using client cookies. If you use the **delete cookie-flag samesite** command to delete the samesite flag in the set-cookie attributes of the response header returned by the Web server, the client can carry the cookie when it sends HTTP or HTTPS requests.
- When the device requests the resources from the Web server, the set-cookie attributes of the HTTP or HTTPS response header returned by the Web server might contain the HTTPOnly flag. If a cookie contains the HTTPOnly flag, the HTTP or HTTPS response header will not carry the cookie when a client requests Web resources by JavaScript, thus making the cookie more secure. However, the user will go offline due to absence of the cookie in the response header. You can use the **delete cookie-flag httponly** command to delete the HTTPOnly flag in the set-cookie attributes of the response header returned by the Web server.

Prerequisites

Configure this feature when the current HTTP proxy server view is not referenced.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Delete response header set-cookie attributes.
delete cookie-flag { httponly | samesite | secure }

By default, the set-cookie attributes in the HTTP or HTTPS response header are not modified.

Enabling the restoration of QueryString in Web requests

About this task

After the external link reference feature is enabled, the QueryString parameters in the URLs of the HTTP or HTTPS request packets sent by the client may contain domain names replaced by the device. By default, the device does not restore the replaced domain names in the QueryString parameters, and thus the client cannot access Web sources through the QueryString parameters. With this feature enabled, the device restores the replaced fields in the QueryString parameters to the original domain name, so as to ensure that the client can obtain the requested resources normally.

Prerequisites

Enable the restoration of QueryString in Web requests when the current HTTP proxy server view is not referenced.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Enable the restoration of QueryString in Web requests.
restore request-querystring
By default, the restoration of QueryString in Web requests is disabled.

Replacing an HTTP or HTTPS response header or restoring an HTTP or HTTPS request header

About this task

By default, the device does not replace the fields in the HTTP or HTTPS response header. After the external link reference feature is enabled, the device can proxy any external links. When the device proxies external links on the Web server with origins outside the server, the client needs to send cross-domain requests. However, some clients do not allow cross-domain requests, so they cannot access external links with origins outside the server. With the **replace response-header** command enabled, the device uses the wildcard domain name specified by the **wildcard-domain-name** command to replace specified fields in an HTTP or HTTPS response header. For example, the device modifies **https://www.abc.com** in the referer field into **http://https-www-abc-com.gov6.cn** (with wildcard domain name **gov6.cn** specified). When the client receives the HTTP or HTTPS response with the replaced response header, it does not consider the access request in the response as a cross-domain request. In this way, it can access external links with origins outside the server.

After the **replace response-header** command is enabled, the device uses the wildcard domain name to replace specified fields in an HTTP or HTTPS response header. When the client sends HTTP or HTTPS requests according to the response from the device, the relevant fields in the request header are the replaced fields. With the **restore request-header** command enabled, the device restores the replaced fields to ensure normal proxy of Web sources.

Prerequisites

To make this feature take effect for an HTTP proxy service, you must specify a wildcard domain name for the HTTP proxy service. For more information, see "[Configuring the external link reference feature](#)" in an HTTP proxy service view.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Enable the replacement of specified fields in an HTTP or HTTPS response header.
replace response-header { access-control-allow-origin | location | p3p | refresh | vary }
By default, the replacement of all fields in an HTTP or HTTPS response header is disabled.
4. Enable the restoration of fields in an HTTP or HTTPS request header.
restore request-header { origin | referer | x-wap-profile }
By default, the restoration of fields in an HTTP or HTTPS request header is disabled.

Configuring a redirect URL domain name that allows replacement

About this task

For an HTTP proxy service with a specified wildcard domain name, if the external link reference feature in an HTTP proxy server view is disabled, by default, the device cannot use configurations in the view to proxy a redirect URL. After you configure this feature, the device will replace the redirect URL domain name in the HTTP or HTTPS response header returned by the Web server. It adds the specified wildcard domain name to the redirect URL domain name to proxy the redirect URL. This feature can be applied in scenarios where the device only needs to proxy part of the external link resources.

Restrictions and guidelines

This feature does not take effect if the external link reference feature in an HTTP proxy server view is enabled.

Prerequisites

To make this feature take effect for an HTTP proxy service, you must specify a wildcard domain name for the HTTP proxy service. For more information, see "[Configuring the external link reference feature](#)" in an HTTP proxy service view.

Procedure

1. Enter system view.
system-view
2. Enter the view of an HTTP proxy server.
http-proxy server *server-name*
3. Configure a redirect URL domain name that allows replacement.
include-redirect-domain *domain-name*
By default, no redirect URL domain name that allows replacement is configured.

Referencing an HTTP proxy server view

About this task

After an HTTP proxy server view is referenced, the device uses the configurations in the HTTP proxy server view to proxy all Web resources on the current slot. The type of referenced HTTP proxy server views is as follows:

- **Non-default HTTP proxy server view**—The configurations in the view can only proxy the Web servers of the allowlist domain names specified by the **domain-name** command.
- **Default HTTP proxy server view**—If the Web resources requested by the client does not match the domain names specified in any HTTP proxy server view, the device will use the configurations in the default HTTP proxy server view for proxy.

Restrictions and guidelines

If the default HTTP proxy server view is not specified in the referenced HTTP proxy server view, the HTTP proxy service cannot be enabled. You can specify only a referenced HTTP proxy server view as the default HTTP proxy server view.

If the **ache-data**, **domain-name**, **extlink-href enable**, **failed-extlink inform**, **failed-extlink redirect**, **medialink-proxy enable**, **hyperlink-proxy**, **ipv6-address**, or **protocol-type** command is configured in an HTTP proxy service view, you cannot reference the HTTP proxy server view.

Prerequisites

Configure reference to an HTTP proxy server view when the HTTP proxy service is disabled. You can enable the HTTP proxy service again after completing the configurations.

Procedure

1. Enter system view.
system-view
2. Create an HTTP proxy service and enter its view.
Centralized devices:
http-proxy service *service-name*
Distributed devices in standalone mode: Centralized IRF devices:
http-proxy service *service-name slot slot-number*
Distributed devices in IRF mode:
http-proxy service *service-name chassis chassis-number slot slot-number*
3. Specify a referenced HTTP proxy server view as the default HTTP proxy server view.
include server *server-name default*
By default, no HTTP proxy server view is referenced in an HTTP proxy service.
4. (Optional.) Specify a referenced HTTP proxy server view as the non-default HTTP proxy server view.
include server *server-name*
By default, no HTTP proxy server view is referenced in an HTTP proxy service.

Enabling wildcard domain name encryption feature for an HTTP proxy service

About this task

With the wildcard domain name encryption feature enabled, in external link proxy, the device uses the specified algorithm to encrypt the external link containing the wildcard domain name. When the client accesses the external link later, the HTTP or HTTPS requests sent by the client carry the encrypted external link. The device will decrypt the link and then proxy the resource, so as to prevent illegal users from forging the wildcard domain name to access the external link and occupying proxy resources.

Restrictions and guidelines

To use this feature in HTTP proxy service view, you must first execute the **include server** command to reference an HTTP proxy server view. To cancel the reference to an HTTP proxy server view, first disable the wildcard domain name encryption feature in the current HTTP proxy service view.

Prerequisites

Before enabling wildcard domain name encryption for an HTTP proxy service, first disable the HTTP proxy service and reference the HTTP proxy server view.

Procedure

1. Enter system view.
system-view
2. Create an HTTP proxy service and enter its view.
Centralized devices:
http-proxy service *service-name*

Distributed devices in standalone mode:Centralized IRF devices:

http-proxy service *service-name* **slot** *slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*

3. Enable wildcard domain name encryption feature for an HTTP proxy service.

extlink-encryption algorithm { **algx** | **algy** | **algz** }

By default, the wildcard domain name encryption feature for an HTTP proxy service is disabled.

Configuring the HTTP proxy operation recording

You can reuse the configurations in an HTTP proxy service view to configure the feature in an HTTP proxy server view. For more information, see "错误!未找到引用源。" in an HTTP proxy service view.

Enabling an HTTP proxy service

1. Enter system view.

system-view

2. Enter the view of an HTTP proxy service.

Centralized devices:

http-proxy service *service-name*

Distributed devices in standalone mode:Centralized IRF devices:

http-proxy service *service-name* **slot** *slot-number*

Distributed devices in IRF mode:

http-proxy service *service-name* **chassis** *chassis-number* **slot** *slot-number*

3. Enable the HTTP proxy service.

service enable

By default, an HTTP proxy service is disabled.

Display and maintenance commands for HTTP proxy in an HTTP proxy server view

Execute **display** commands in any view.

Task	Command
Display configuration information in an HTTP proxy service view.	display http-proxy { server-group [<i>group-name</i>] service [<i>service-name</i>] }
Display configuration information in an HTTP proxy server view.	display http-proxy server server-name

Command reference

Modified command: cache-data

Use **cache-data** to enable the device to cache Web server resources and specify the directory for storing cache files.

Use **undo cache-data** to disable the device from caching Web server resources.

Syntax

cache-data directory *directory*

undo cache-data

Views

HTTP proxy service view

HTTP proxy server view

Change description

The default for this command has changed:

- Before modification:
The device does not cache Web server resources
- After modification:
The device does not cache Web server resources and the directory for storing cache files is not specified.

The **cache-data** command is added to HTTP proxy server view.

The usage guidelines for this command have changed:

- Before modification:
Before changing the cache file directory for an HTTP proxy service, make sure the HTTP proxy service is disabled.
If you execute this command multiple times, the most recent configuration takes effect.
Currently, the device can cache the apk, bmp, doc, docx, gif, gzip, ipa, jar, jpg, jpeg, mp4, pdf, png, pptx, rar, swf, tar, txt, xls, xlsx, or zip files on the webpages.
- After modification:
If you want to reference an HTTP proxy server in an HTTP proxy service, when you execute this command for the HTTP proxy server, the specified directory path must be the path of the slot where the HTTP proxy service is located. Otherwise, the reference will fail.
Before changing the cache file directory for an HTTP proxy service, make sure the HTTP proxy service is disabled. Before changing the cache file directory for an HTTP proxy server, make sure the HTTP proxy server is not referenced.
If you execute this command multiple times, the most recent configuration takes effect.
Currently, the device can cache the apk, bmp, doc, docx, gif, gzip, ipa, jar, jpg, jpeg, mp4, pdf, png, pptx, rar, swf, tar, txt, xls, xlsx, or zip files on the webpages.
Do not use this command in an HTTP proxy service view after the HTTP proxy service references an HTTP proxy server.

New command: delete cookie-flag

Use **delete cookie-flag** to delete a Set-Cookie attribute from an HTTP/HTTPS response.

Use **undo delete cookie-flag** to restore the default.

Syntax

```
delete cookie-flag { httponly | samesite | secure }  
undo delete cookie-flag { httponly | samesite | secure }
```

Default

The device does not modify the Set-Cookie attributes in an HTTP or HTTPS response.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

httponly: Specifies the HTTPOnly attribute in a cookie.

samesite: Specifies the SameSite attribute in a cookie.

secure: Specifies the Secure attribute in a cookie.

Usage guidelines

After the external link reference feature is enabled in an HTTP proxy server view, the device will add a wildcard domain name to the external link URL in the response returned by the Web server and modify the external link URL into HTTP format. For example, the device modifies external link URL **https://abc.com** into **http://https-abc-com.gov6.cn** by adding wildcard domain name **gov6.cn**. A client sends an HTTP request containing the wildcard domain name to the device when it accesses the external link. After the device receives the HTTP request, it restores the external link URL in the request to **https://abc.com** and then sends the request to the Web server through HTTPS.

In the previous process, the Web server returns an HTTPS response, and the Set-Cookie header in the response might contain the Secure attribute. The Secure attribute requires a secure transmission of a cookie through HTTPS to improve the security of the cookie. Because the client requests external link resources through HTTP, it does not save the cookie with the Secure attribute. As a result, the user will go offline when it accesses the external link resources. To avoid this issue, you can execute the **delete cookie-flag secure** command. The Secure attribute in a Set-Cookie header returned by the Web server will be deleted, so the client will save the cookie.

For high security purpose, a Web server will carry the SameSite attribute for the cookie in a Set-Cookie header of an HTTP or HTTPS response. The SameSite attribute is used to restrict third-party cookies and prevents illegal websites from forging HTTP or HTTPS requests by using client cookies. After a client saves a cookie with the SameSite attribute, it regards the device enabled with the HTTP proxy service as a third-party website and therefore does not carry the cookie in the HTTP/HTTPS request sent to the device. For the client to send the cookie in the HTTP/HTTPS request, you can execute the **delete cookie-flag same-site** command to configure the device to delete the SameSite attribute from the Set-Cookie headers in HTTP/HTTPS responses returned from the Web server.

When the device requests resources from a Web server, the Set-Cookie header in the HTTP or HTTPS response returned by the Web server might contain the HTTPOnly attribute, which forbids JavaScript from accessing the cookie. After a client saves a cookie containing the HTTPOnly attribute, the client will not carry the cookie in the HTTP/HTTPS requests when it requests Web resources by JavaScript. The user will go offline due to absence of the cookie in the HTTP/HTTPS request header. In scenarios that need to retain the user status, you can use the **delete cookie-flag httponly** command to configure the device to delete the HTTPOnly attribute from the Set-Cookie response headers returned by the Web server.

You can execute this command multiple times to configure the device to delete multiple Set-Cookie attributes.

Execute this command for an HTTP proxy server when it is not referenced by an HTTP proxy service.

Examples

Configure HTTP proxy server **test** to delete the Secure attribute from Set-Cookie HTTP/HTTPS headers.

```
<Sysname> system-view
[Sysname] http-proxy server test
[Sysname-http-proxy-server-test] delete cookie-flag secure
```

Related commands

http-proxy server

service enable

Modified command: denylist-domain-name

Use **denylist-domain-name** to specify a denylist domain name for an HTTP proxy service.

Use **undo denylist-domain-name** to delete a denylist domain name for an HTTP proxy service.

Syntax

denylist-domain-name *domain-name*

undo denylist-domain-name *domain-name*

Views

HTTP proxy service view

Change description

The description for the *domain-name* argument has changed:

- Before modification:
domain-name: Specifies a denylist domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).
- After modification:
domain-name: Specifies a denylist domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. You can enter three to five such suffixes. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), dots (.), and asterisk (*). The asterisk (*) character is used to match the domain names with fixed starting or ending string. For example, **www.test.*** represents all domain names starting with **www.test.**; ***.test.gov** represents all domain names ending with **.test.gov**.

Modified command: display http-proxy

Use **display http-proxy** to display HTTP proxy configuration information.

Syntax

display http-proxy { **server-group** [*group-name*] | **service** [*service-name*] }

Views

Any view

Change description

The case sensitivity for the *group-name* and *service-name* arguments has changed:

- Before modification:

group-name: Specifies a Web server group by its name, a case-insensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_). If you do not specify a Web server group, this command displays configuration information about all Web server groups.

service-name: Specifies an HTTP proxy service by its name, a case-insensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_). If you do not specify an HTTP proxy service, this command displays configuration information about all HTTP proxy services.

- After modification:

group-name: Specifies a Web server group by its name, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_). If you do not specify a Web server group, this command displays configuration information about all Web server groups.

service-name: Specifies an HTTP proxy service by its name, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_). If you do not specify an HTTP proxy service, this command displays configuration information about all HTTP proxy services.

The following fields are added to the output for this command:

Table 81 Command output

Field	Description
Include Server	HTTP proxy server view referenced by the HTTP proxy service. This field displays N/A if no HTTP proxy server view is referenced.
Extlink encryption algorithm	Algorithm used in wildcard domain name encryption for an HTTP proxy service. This field displays N/A if no algorithm is specified.

New command: display http-proxy server

Use **display http-proxy server** to display the configuration for an HTTP proxy server.

Syntax

display http-proxy server *server-name*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-name: Specifies an HTTP proxy server by its name, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_).

Examples

Display the configuration for HTTP proxy server **test**.

```
[Sysname]display http-proxy server test
Server name: test
IPv6 address:                2001::1
Allowlist domain names:      www.abcd.com
Protocol types:              HTTP at port 8000
Failed extlink error codes:   N/A
Excluded external domain name: N/A
Restore request header name:  N/A
Replace response header name: N/A
Include external domain name: N/A
Include redirect domain name: N/A
Referer protection domain name: N/A
    Allowlist:                N/A
Delete cookie flag:          secure
Restore request querystring: Disabled
Extlink href:                Disabled
Failed extlink inform:       Disabled
Cache data:                  Disabled
    Cache file path:          N/A
```

Table 82 Command output

Field	Description
Server name	Name of an HTTP proxy server.
IPv6 address	IPv6 address configured in the HTTP proxy server view. This field displays N/A if no IPv6 address is configured.
Allowlist Domain name	Allowlist domain name configured in the HTTP proxy server view. This field displays N/A if no allowlist domain name is configured.
Protocol types	Protocol types and listening port number specified for the HTTP proxy service in the HTTP proxy server view. This field displays N/A if no protocol types and listening port number are specified.
Failed extlink error codes	Error codes for the external link proxying failure configured in the HTTP proxy server view. This field displays N/A if no error code is configured for the external link proxying failure.
Excluded external domain name	Domain name of the external link to be not proxied by the HTTP proxy service configured in the HTTP proxy server view. This field displays N/A if you have not specified the external link domain name to be not proxied by the HTTP proxy service.
Restore request header name	Fields in the request header to be restored configured in the HTTP proxy server view. The field displays N/A if no fields in the request header to be restored are configured.
Replace response header name	Fields in the response header to be replaced configured in the HTTP proxy server view. The field displays N/A if no fields in the response header to be replaced are

	configured.
Include external domain name	Domain name of the external link to be proxied configured in the HTTP proxy server view. The field displays N/A if the domain name of an external link to be proxied is not configured.
Include redirect domain name	Redirect URL domain name that allows replacement configured in the HTTP proxy server view. The field displays N/A if a redirect URL domain name that allows replacement is not configured.
Referer protection domain name	Domain name of the proxied external link with external link reference feature enabled by the device in the HTTP proxy server view. The field displays N/A if the domain name of a proxied external link with enabled referer protection feature is not configured.
Allowlist	Referer allowlist. The field displays N/A if no referer allowlist is configured.
Delete cookie flag	Flag in the response header set-cookie attributes to be deleted configured in the HTTP proxy server view. The field displays N/A if a flag in the response header set-cookie attributes to be deleted is not configured.
Restore request querystring	Status of the querystring restoration feature configured in the HTTP proxy server view: • Enabled. • Disabled.
Extlink href	External link reference status configured in the HTTP proxy server view: • Enabled. • Disabled.
Failed extlink inform	Status of the external link proxying failure informing feature configured in the HTTP proxy server view: • Enabled. • Disabled.
Cache data	Web resource caching status configured in the HTTP proxy server view: • Enabled. • Disabled.
Cache file path	Path for saving the cache files. This field displays N/A if no cache file path is specified.

Modified command: domain-name

Use **domain-name** to specify an allowlist domain name for an HTTP proxy service.

Use **undo domain-name** to delete an allowlist domain name for an HTTP proxy service.

Syntax

domain-name *domain-name*

undo domain-name *domain-name*

Views

HTTP proxy service view

HTTP proxy server view

Change description

This command is added to HTTP proxy server view.

The description for the *domain-name* argument has changed:

- Before modification:
domain-name: Specifies an allowlist domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).
- After modification:
domain-name: Specifies an allowlist domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. You can enter three to five such suffixes. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), dots (.), and asterisk (*). The asterisk (*) character is used to match a series of domain names with fixed starting or ending string. For example, **www.test.*** represents all domain names starting with **www.test.**; ***.test.gov** represents all domain names ending with **.test.gov**.

The usage guidelines for this command has changed:

- Before modification:
After you configure allowlist domain names, when a client tries to access a website through the proxy service, the device returns an error page to the client if the domain name of the requested website is not in the allowlist.
If you have not configured the wildcard domain name or enabled external link reference for an HTTP proxy service, the device responds a new domain name to a client who requests to access an external link on a Web server. The new domain name is composed of the domain name specified by this command plus the domain name of the external link. Thus, the device can use the specified DNS server to resolve new domain name into the IP address of the server that stores the external link resource. For a client, the domain name specified by this command must be the same as the domain name of the Web server accessed by the client.
For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.
A maximum of 512 allowlist domain names can be configured in a view. You can execute this command multiple times to configure multiple allowlist domain names.
A domain name can only be added to the domain name allowlist or the domain name denylist. The **denylist-domain-name** and **domain-name** commands are mutually exclusive.
Before specifying an allowlist domain name for an HTTP proxy service, first disable the HTTP proxy service.
- After modification:
After you configure allowlist domain names, when a client tries to access a website through the proxy service, the device returns an error page to the client if the domain name of the requested website is not in the allowlist.
If you have not configured the wildcard domain name or enabled external link reference for an HTTP proxy service, the device responds a new domain name to a client who requests to access an external link on a Web server. The new domain name is composed of the domain name specified by this command plus the domain name of the external link. Thus, the device can use the specified DNS server to resolve new domain name into the IP address of the server that stores the external link resource. For a client, the domain name specified by this command must be the same as the domain name of the Web server accessed by the client. The proxy service configured in HTTP proxy server view cannot proxy an external link by using the domain name specified by this command plus the domain name of the external link.

For more information about external link, see HTTP proxy configuration in *Layer 3—IP Services Configuration Guide*.

A maximum of 512 allowlist domain names can be configured in a view. You can execute this command multiple times to configure multiple allowlist domain names.

A domain name can only be added to the domain name allowlist or the domain name denylist. The **denylist-domain-name** and **domain-name** commands are mutually exclusive.

Before specifying an allowlist domain name for an HTTP proxy service, first disable the HTTP proxy service. Before specifying an allowlist domain name for an HTTP proxy server, make sure the HTTP proxy server is not referenced.

You cannot execute this command for an HTTP proxy service that has referenced an HTTP proxy server.

Modified command: exclude-external-domain

Use **exclude-external-domain** to specify an external link domain name not to be proxied by an HTTP proxy service, hereinafter referred to as excluded external domain name.

Use **undo exclude-external-domain** to remove an excluded external domain name.

Syntax

exclude-external-domain *domain-name*

undo exclude-external-domain *domain-name*

Views

HTTP proxy service view

HTTP proxy server view

Change description

This command is added to HTTP proxy server view.

The usage guidelines for this command have changed:

- Before modification:

Before specifying an excluded external domain name for an HTTP proxy service, disable the HTTP proxy service.

A maximum of 512 external link domain names can be configured. You can execute this command multiple times to configure multiple external link domain names.
- After modification:

Before specifying an excluded external domain name for an HTTP proxy service, disable the HTTP proxy service. Before specifying an excluded external domain name for an HTTP proxy server, make sure the HTTP proxy server is not referenced.

A maximum of 512 external link domain names can be configured in a view. You can execute this command multiple times to configure multiple external link domain names.

New command: extlink-encryption algorithm

Use **extlink-encryption algorithm** to enable wildcard domain name encryption feature for an HTTP proxy service.

Use **undo extlink-encryption algorithm** to disable wildcard domain name encryption feature for an HTTP proxy service.

Syntax

extlink-encryption algorithm { **algx** | **algy** | **algz** }

undo extlink-encryption algorithm { algx | algy | algz }

Default

The wildcard domain name encryption feature for an HTTP proxy service is disabled.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

algx: Specifies algorithm x.

algy: Specifies algorithm y.

algz: Specifies standard MD5 algorithm.

Usage guidelines

With the wildcard domain name encryption feature enabled, in external link proxy, the device uses the specified algorithm to encrypt the external link containing the wildcard domain name. When the client accesses the external link later, the HTTP or HTTPS requests sent by the client carry the encrypted external link. The device will decrypt the link and then proxy the resource, so as to prevent illegal users from forging the wildcard domain name to access the external link and occupying proxy resources.

Enable wildcard domain name encryption for an HTTP proxy service when the HTTP proxy service is disabled.

To enable wildcard domain name encryption for an HTTP proxy service, make sure the HTTP proxy service has referenced an HTTP proxy server by using the **include server** command. To cancel the reference to an HTTP proxy server, first disable wildcard domain name encryption for the current HTTP proxy service.

Examples

(Centralized devices.) Use algorithm x to encrypt the wildcard domain name of an HTTP proxy service.

```
<Sysname> system-view
```

```
[Sysname] http-proxy service test
```

```
[Sysname-http-proxy-service-test] extlink-encryption algorithm algx
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Use algorithm x to encrypt the wildcard domain name of an HTTP proxy service on slot 1.

```
<Sysname> system-view
```

```
[Sysname] http-proxy service test slot 1
```

```
[Sysname-http-proxy-service-test-slot1] extlink-encryption algorithm algx
```

Related commands

service enable

Modified command: extlink-href enable

Use **extlink-href enable** to enable external link reference for an HTTP proxy service.

Use **undo extlink-href enable** to disable external link reference for an HTTP proxy service.

Syntax

extlink-href enable

undo extlink-href enable

Views

HTTP proxy service view

HTTP proxy server view

Change description

This command is added to HTTP proxy server view.

The usage guidelines for this command have changed:

- Before modification:

After you configure a wildcard domain name and enable the external link reference feature, the device will add the specified wildcard domain name to the external link domain name that is requested by a client.

Before enabling external link reference for an HTTP proxy service, first disable the HTTP proxy service.
- After modification:

After you configure a wildcard domain name and enable the external link reference feature, the device will add **http://** and the specified wildcard domain name to the external link domain name that is requested by a client.

Before enabling external link reference for an HTTP proxy service, first disable the HTTP proxy service. Before enabling external link reference for an HTTP proxy server, make sure the HTTP proxy server is not referenced.

You cannot execute this command for an HTTP proxy service that has referenced an HTTP proxy server.

Modified command: failed-extlink inform

Use **failed-extlink inform** to enable the external link proxying failure informing feature.

Use **undo failed-extlink inform** to disable the external link proxying failure informing feature.

Syntax

failed-extlink inform

undo failed-extlink inform

Views

HTTP proxy service view

HTTP proxy server view

Change description

This command is added to HTTP proxy server view.

The usage guidelines for this command have changed:

- Before modification:

Before enabling external link proxying failure informing for an HTTP proxy service, first disable the HTTP proxy service.
- After modification:

Before enabling external link proxying failure informing for an HTTP proxy service, first disable the HTTP proxy service. Before enabling external link proxying failure informing for an HTTP proxy server, make sure the HTTP proxy server is not referenced.

You cannot execute this command for an HTTP proxy service that has referenced an HTTP proxy server.

Modified command: failed-extlink redirect

Use **failed-extlink redirect** to enable the external link proxying failure redirection feature.

Use **undo failed-extlink redirect** to disable the external link proxying failure redirection feature.

Syntax

failed-extlink redirect *error-code*

undo failed-extlink redirect *error-code*

Views

HTTP proxy service view

HTTP proxy server view

Change description

This command is added to HTTP proxy server view.

The usage guidelines for this command have changed:

- Before modification:
Before enabling external link proxying failure redirection for an HTTP proxy service, first disable the HTTP proxy service.
- After modification:
Before enabling external link proxying failure redirection for an HTTP proxy service, first disable the HTTP proxy service. Before enabling external link proxying failure redirection for an HTTP proxy server, make sure the HTTP proxy server is not referenced.
You cannot execute this command for an HTTP proxy service that has referenced an HTTP proxy server.

Modified command: http-proxy server-group

Use **http-proxy server-group** to create a Web server group and enter its view, or enter the view of an existing Web server group.

Use **undo http-proxy server-group** to delete a Web server group.

Syntax

http-proxy server-group *group-name*

undo http-proxy server-group *group-name*

Views

System view

Change description

The case sensitivity for the *group-name* argument has changed:

- Before modification:
group-name: Specifies the name of the Web server group, a case-insensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_).
- After modification:
group-name: Specifies the name of the Web server group, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_).

New command: http-proxy server

Use **http-proxy server** to create an HTTP proxy server and enter its view, or enter an existing HTTP proxy server view.

Use **undo http-proxy server** to delete an HTTP proxy server and all the configurations in the HTTP proxy server view.

Syntax

http-proxy server *server-name*

undo http-proxy server *server-name*

Default

No HTTP proxy servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

service-name: Specifies an HTTP proxy server name, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_).

Usage guidelines

You can configure HTTP proxy service settings in both HTTP proxy service view and HTTP proxy server view. The settings in HTTP proxy service view apply to all the Web servers on the device, IRF member device, or card. The settings in HTTP proxy server view apply only to the specified Web server resources. An HTTP proxy server view has smaller granularity and higher flexibility. Using HTTP proxy servers, you can configure different proxy configurations for different Web server resources according to the requirements of users or Web servers.

The settings in an HTTP proxy service view also take effect on the HTTP proxy server. To delete an HTTP proxy server, first execute the **undo include server** command to cancel the reference to the HTTP proxy server, and then execute the **undo http-proxy server** command to delete the server.

Examples

Create HTTP proxy server **test** and enter its view.

```
<Sysname> system-view
```

```
[Sysname] http-proxy server test
```

```
[Sysname-http-proxy-server-test]
```

Related commands

domain-name

include server

Modified command: hyperlink-proxy

Use **hyperlink-proxy** to specify an external link to be proxied by an HTTP proxy service.

Use **undo hyperlink-proxy** to remove an external link from the external hyperlinks proxied by an HTTP proxy service.

Syntax

hyperlink-proxy *link-string*

undo hyperlink-proxy *link-string*

Views

HTTP proxy service view

Change description

The following usage guidelines for this command are added:

You cannot execute this command for an HTTP proxy service that has referenced an HTTP proxy server.

New command: include-external-domain

Use **include-external-domain** to configure an external link domain name in an HTTP proxy server view.

Use **undo include-external-domain** to delete the configurations for the external link domain name in the HTTP proxy server view.

Syntax

include-external-domain *domain-name*

undo include-external-domain [*domain-name*]

Default

No external link domain name is configured in an HTTP proxy server view.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an external link domain name in the HTTP proxy server view. In format, **http://** or **https://** is added before the specified domain name. The domain name suffix is a dot-separated string, for example, **aabbcc.com**. Each separated string includes no more than 63 characters. You can enter a minimum of three such strings or a maximum of five such strings. The domain name is a case-insensitive string, including a maximum of 253 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

For an HTTP proxy service with a specified wildcard domain name, if the external link reference feature in an HTTP proxy server view is disabled, by default, the device cannot use configurations in the view to proxy an external link. After you configure this command, the device will replace the external link domain name specified by the *domain-name* argument in the HTTP or HTTPS response header returned by the Web server. It adds the specified wildcard domain name to the external link domain name to proxy the specified external link. This command can be applied in scenarios where the device only needs to proxy part of the external link resources.

This command does not take effect if the external link reference feature in an HTTP proxy server view is enabled.

A maximum of 512 external link domain names can be configured in an HTTP proxy server view. You can execute this command multiple times to configure multiple external link domain names.

Execute this command when the current HTTP proxy server view is not referenced.

Examples

Configure external link domain name **test.gov.cn** in HTTP proxy server view **test**.

```
<Sysname> system-view
[Sysname] http-proxy server test
[Sysname-http-proxy-server-test] include-external-domain http://test.gov.cn
```

Related commands

extlink-external-domain

http-proxy server

service enable

wildcard-domain-name

New command: include-redirect-domain

Use **include-redirect-domain** to configure a redirect URL domain name that allows replacement in an HTTP proxy server view.

Use **undo include-redirect-domain** to delete the configurations for the redirect URL domain name that allows replacement in the HTTP proxy server view.

Syntax

include-redirect-domain *domain-name*

undo include-redirect-domain [*domain-name*]

Default

No redirect URL domain name that allows replacement is configured in an HTTP proxy server view.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a redirect URL domain name that allows replacement. In format, **http://** or **https://** is added before the specified domain name. The domain name suffix is a dot-separated string, for example, **aabbcc.com**. Each separated string includes no more than 63 characters. You can enter a minimum of three such strings or a maximum of five such strings. The domain name is a case-insensitive string, including a maximum of 253 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).

Usage guidelines

For an HTTP proxy service with a specified wildcard domain name, if the external link reference feature in an HTTP proxy server view is disabled, by default, the device cannot use configurations in the view to proxy a redirect URL. After you configure this command, the device will replace the redirect URL domain name specified by the *domain-name* argument in the HTTP or HTTPS response header returned by the Web server. It adds the specified wildcard domain name to the redirect URL domain name to proxy the redirect URL. This command can be applied in scenarios where the device only needs to proxy part of the external link resources.

This command does not take effect if the external link reference feature in an HTTP proxy server view is enabled.

You can execute this command multiple times to configure multiple redirect URL domain names that allow replacement.

Execute this command when the current HTTP proxy server view is not referenced.

Examples

```
# Configure redirect URL domain name test.gov.cn to be replaced in HTTP proxy server view test.
<Sysname> system-view
[Sysname] http-proxy server test
[Sysname-http-proxy-server-test] include-redirect-domain http://tyrz.gxzf.gov.cn
```

Related commands

extlink-external-domain
http-proxy server
service enable
wildcard-domain-name

New command: include server

Use **include server** to reference an HTTP proxy server.

Use **undo include server** to cancel the reference to an HTTP proxy server.

Syntax

```
include server server-name [ default ]
undo include server server-name
```

Default

No HTTP proxy server is referenced in an HTTP proxy service.

Views

HTTP proxy service view

Predefined user roles

network-admin

Parameters

service-name: Specifies an HTTP proxy server view by its name, a case-sensitive string of 1 to 63 characters. The name can include digits, letters, and underscores (_).

default: Specifies the default HTTP proxy server view for reference. Only an HTTP proxy server view can be specified as the default HTTP proxy server view. If you do not specify this keyword, non-default HTTP proxy server views are specified the HTTP proxy server views for reference.

Usage guidelines

The device will use the configurations in the HTTP proxy server view to proxy the domain name Web resources specified by the **domain-name** command, if you perform the following operations:

- Execute the **domain-name** command in an HTTP proxy server view.
- Execute the **include server** command to reference the HTTP proxy server view in an HTTP proxy service view.

After the default HTTP proxy server view is referenced, if the Web resources requested by the client does not match the domain names specified in any HTTP proxy server view, the device will use the configurations in the default HTTP proxy server view for proxy.

Configure reference to an HTTP proxy server view when the HTTP proxy service is disabled. If the default HTTP proxy server view is not specified in the referenced HTTP proxy server view, the HTTP proxy service cannot be enabled.

If the **ache-data**, **domain-name**, **extlink-href enable**, **failed-extlink inform**, **failed-extlink redirect**, **medialink-proxy enable**, **hyperlink-proxy**, **ipv6-address**, or **protocol-type** command is configured in an HTTP proxy service view, you cannot reference the HTTP proxy server view.

Examples

(Centralized devices.) Specify HTTP proxy server view **server1**.

```
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] include server server1
```

(Centralized IRF devices.) (Distributed devices in standalone mode.) Specify HTTP proxy server view **server1** on slot 1.

```
<Sysname> system-view
[Sysname] http-proxy service test slot 1
[Sysname-http-proxy-service-test-slot1] include server server1
```

Related commands

service enable

http-proxy server

Modified command: ipv6-address

Use **ipv6-address** to specify an IPv6 address for an HTTP proxy service.

Use **undo ipv6-address** to delete the IPv6 address for an HTTP proxy service.

Syntax

ipv6-address *ipv6-address*

undo ipv6-address

Views

HTTP proxy service view

HTTP proxy server view

Change description

This command is added to HTTP proxy server view.

The usage guidelines for this command have changed:

- Before modification:
Before specifying an IPv6 address for an HTTP proxy service, first disable the HTTP proxy service.
- After modification:
Before specifying an IPv6 address for an HTTP proxy service, first disable the HTTP proxy service and ensure that the current HTTP proxy server view is not referenced.
Do not use this command in an HTTP proxy service view after an HTTP proxy server view is referenced.

Modified command: medialink-proxy enable

Use **medialink-proxy enable** to enable the external media link proxy feature for an HTTP proxy service.

Use **undo medialink-proxy enable** to disable the external media link proxy feature for an HTTP proxy service.

Syntax

medialink-proxy enable

undo medialink-proxy enable

Default

The external media link proxy feature for an HTTP proxy service is disabled.

Views

HTTP proxy service view

Change description

The following usage guidelines for this command are added:

Do not use this command when the current HTTP proxy service view references an HTTP proxy server view.

Modified command: protocol-type (http proxy service view)

Use **protocol-type** to specify a protocol type and listening port number for an HTTP proxy service and bind a Web server group to the service.

Use **undo protocol-type** to delete the protocol and listening port settings for an HTTP proxy service and unbind the Web server group from the service.

Syntax

protocol-type { **http** | **https** } [**port** *port-number*] [**server-group** *group-name*]

undo protocol-type { **http** | **https** } [**port** *port-number*] [**server-group** *group-name*]

Views

HTTP proxy service view

Change description

The usage guidelines for this command have changed:

- Before modification:
To access different Web servers, you can execute this command multiple times to configure multiple listening ports and Web server groups for an HTTP proxy service.
- After modification:
To access different Web servers, you can execute this command multiple times to configure multiple listening ports and Web server groups for an HTTP proxy service. If you execute this command multiple times for a listening port, the most recent configuration takes effect.
Do not use this command when an HTTP proxy server view is referenced. Execute this command when an HTTP proxy service is disabled.

New command: protocol-type (HTTP proxy server view)

Use **protocol-type** to specify a protocol type and listening port number for an HTTP proxy service in an HTTP proxy server view.

Use **undo protocol-type** to delete the protocol and listening port settings for the HTTP proxy service in the HTTP proxy server view.

Syntax

```
protocol-type { http | https } [ port port-number ]  
undo protocol-type { http | https } [ port port-number ]
```

Default

No protocol type or listening port number is specified for an HTTP proxy service in an HTTP proxy server view.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

http: Specifies the HTTP protocol.

https: Specifies the HTTPS protocol.

port port-number: Specifies the port number on which the HTTP proxy service listens. The value range is 1 to 65535. The default listening port number for the HTTP protocol and HTTPS protocol is 80 and 443, respectively.

Usage guidelines

With this command configured, if an IPv6 client uses the specified protocol and port number to access a Web server:

- For an IPv6 Web server, the device directly forwards the IPv6 packets received from the client to the Web server.
- For an IPv4 Web server, the device first converts the IPv6 packets of the client to IPv4 packets. Then the device uses the specified protocol to encapsulate the packets before sending them to the specified Web server.

The protocol type and port number supported by an HTTP proxy service must match those in an HTTP or HTTPS request of an IPv6 client.

You can execute this command multiple times to configure multiple listening ports for an HTTP proxy service. If you execute this command multiple times for a listening port, the most recent configuration takes effect.

Execute this command when the current HTTP proxy server view is not referenced.

Examples

Specify HTTP and port number 8000 as the protocol type and listening port number of an HTTP proxy service in HTTP proxy server view **test**.

```
<Sysname> system-view  
[Sysname] http-proxy server test  
[Sysname-http-proxy-server-test] protocol-type http port 8000
```

Related commands

http-proxy server

include server

New command: referer-protection domain

Use **referer-protection domain** to configure a referer allowlist domain name.

Use **undo referer-protection domain** to delete the configurations for the referer allowlist domain name.

Syntax

referer-protection domain *domain-name* **allowlist** *allowlist-domain-name*

undo referer-protection domain *domain-name* [**allowlist** *allowlist-domain-name*]

Default

No referer allowlist domain name is configured.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a domain name proxied in HTTP proxy service. The domain name suffix is a dot-separated string, for example, **aabbcc.com**. Each separated string includes no more than 63 characters. You can enter a minimum of three such strings or a maximum of five such strings. The domain name is a case-insensitive string, including a maximum of 253 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).

allowlist-domain-name: Specifies a referer allowlist domain name. The domain name suffix is a dot-separated string, for example, **aabbcc.com**. Each separated string includes no more than 63 characters. You can enter a minimum of three such strings or a maximum of five such strings. The domain name is a case-insensitive string. The maximum number of characters that can be entered varies by device models. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), dots (.), and asterisk (*). The asterisk (*) character is used to match a series of domain names with fixed starting or ending string. For example, **www.test.*** includes all domain names starting with **www.test.**; ***.test.gov** includes all domain names ending with **.test.gov**.

Usage guidelines

With the referer allowlist domain names configured, the referer protection feature is enabled in domain name proxy. When a client accesses a domain name, if the domain name in the referer request header of the sent HTTP or HTTPS request packets is not in the domain name allowlist, the device will deny the requests. The referer protection feature prevents other websites from stealing webpage resources of the proxied Web servers.

You can execute this command multiple times to configure multiple referer allowlist domain names for a proxied domain name. If you execute both the **referer-protection domain** command and the **referer-protection enable** command, the referer request header in the sent HTTP or HTTPS request packets needs to meet the requirements of both commands. Otherwise, the requests are denied.

Execute this command when the current HTTP proxy server is not referenced.

Examples

In HTTP proxy server view **test**, enable referer protection for domain name **test.gov.cn**, and configure referer allowlist domain name **test1.gov.cn**.

```
<Sysname> system-view
[Sysname] http-proxy server test
[Sysname-http-proxy-server-test] referer-protection domain test.gov.cn whitelist
test1.gov.cn
```

Related commands

http-proxy server

referer-protection enable

service enable

New command: replace response-header

Use **replace response-header** to enable the replacement of specified fields in an HTTP or HTTPS response header.

Use **undo replace response-header** to disable the replacement of specified fields in an HTTP or HTTPS response header.

Syntax

```
replace response-header { access-control-allow-origin | location | p3p | refresh | vary }
```

```
undo replace response-header { access-control-allow-origin | location | p3p | refresh | vary }
```

Default

The replacement of all fields in an HTTP or HTTPS response header is disabled.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

access-control-allow-origin: Specifies the access-control-allow-origin field in a response header.

location: Specifies the location field in a response header.

p3p: Specifies the p3p field in a response header.

refresh: Specifies the refresh field in a response header.

vary: Specifies the vary field in a response header.

Usage guidelines

By default, the device does not replace the fields in the HTTP or HTTPS response header. After the external link reference feature is enabled, the device can proxy any external links. When the device proxies external links on the Web server with origins outside the server, the client needs to send cross-domain requests. However, some clients do not allow cross-domain requests, so they cannot access external links with origins outside the server. With the **replace response-header** command enabled, the device uses the wildcard domain name specified by the **wildcard-domain-name** command to replace specified fields in an HTTP or HTTPS response header. For example, the device modifies **https://www.abc.com** in the referer field into **http://https-www-abc-com.gov6.cn** (with wildcard domain name **gov6.cn** specified). When the client receives the HTTP or HTTPS response with the replaced response header, it does not consider the access request in the response as a cross-domain request. In this way, it can access external links with origins outside the server.

You can execute this command multiple times to configure multiple fields to be replaced in an HTTP or HTTPS response header.

Specify the access-control-allow-origin field in the response header when the current HTTP proxy server view is not referenced.

Examples

```
# Specify the access-control-allow-origin field in a response header in HTTP proxy server view test.
```

```
<Sysname> system-view
[Sysname] http-proxy server test
[Sysname-http-proxy-server-test] restore response-header access-control-allow-origin
```

Related commands

extlink-href enable
http-proxy server
service enable
wildcard-domain-name

New command: restore request-header

Use **restore request-header** to enable the restoration of fields in an HTTP or HTTPS request header.

Use **undo restore request-header** to disable the restoration of fields in the HTTP or HTTPS request header.

Syntax

```
restore request-header { origin | referer | x-wap-profile }
undo restore request-header { origin | referer | x-wap-profile }
```

Default

The restoration of fields in an HTTP or HTTPS request header is disabled.

Views

HTTP proxy server view

Predefined user roles

network-admin

Parameters

origin: Specifies the origin field in a request header.
referer: Specifies the referer field in a request header.
x-wap-profile: Specifies the x-wap-profile field in a request header.

Usage guidelines

After the **replace response-header** command is enabled, the device uses the wildcard domain name to replace specified fields in an HTTP or HTTPS response header. When the client sends HTTP or HTTPS requests according to the response from the device, the relevant fields in the request header are the replaced fields. With the **restore request-header** command enabled, the device restores the replaced fields to ensure normal proxy of Web sources.

You can execute this command multiple times to configure multiple fields to be restored in an HTTP or HTTPS request header.

Specify the origin field in a request header when the current HTTP proxy server view is not referenced.

Examples

```
# Specify the origin field in a request header in HTTP proxy server view test.
<Sysname> system-view
[Sysname] http-proxy server test
[Sysname-http-proxy-server-test] restore request-header origin
```

Related commands

http-proxy server
service enable
wildcard-domain-name

New command: restore request-querystring

Use **restore request-querystring** to enable the restoration of QueryString in Web requests.

Use **undo restore request-querystring** to disable the restoration of QueryString in Web requests.

Syntax

restore request-querystring
undo restore request-querystring

Default

The restoration of QueryString in Web requests is disabled.

Views

HTTP proxy server view

Predefined user roles

network-admin

Usage guidelines

After the external link reference feature is enabled, the QueryString parameters in the URLs of the HTTP or HTTPS request packets sent by the client may contain domain names replaced by the device. By default, the device does not restore the replaced domain names in the QueryString parameters, and thus the client cannot access Web sources through the QueryString parameters. With this command enabled, the device restores the replaced fields in the QueryString parameters to the original domain name, so as to ensure that the client can obtain the requested resources normally.

Execute this command when the current HTTP proxy server view is not referenced.

Examples

Enable the restoration of QueryString in Web requests in HTTP proxy server view **test**.

```
<Sysname> system-view  
[Sysname] http-proxy server test  
[Sysname-http-proxy-server-test] restore request-querystring
```

Related commands

extlink-href enable
http-proxy server
service enable
wildcard-domain-name

Modified command: **ssl certificate domain-name file key-file**

Use **ssl certificate domain-name file key-file** to specify an SSL certificate file and SSL certificate key file for an HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.

Use **undo ssl certificate domain-name** to delete the specified SSL certificate file and SSL certificate key file for an HTTP proxy service to allow it to proxy the HTTPS requests for a specific domain name.

Syntax

ssl certificate domain-name *domain-name* **file** *certificate-file* **key-file** *key-file*

undo ssl certificate domain-name *domain-name*

Views

HTTP proxy service view

Change description

The description for the *domain-name* argument has changed:

- Before modification:
domain-name: Specifies a domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), and dots (.).
- After modification:
domain-name: Specifies a domain name, a case-insensitive string with a maximum of 253 characters. The domain name can include dot-separated domain name suffixes (**aabbcc.com**, for example). Each domain name suffix can contain a maximum of 63 characters. You can enter a minimum of three such suffixes or a maximum of five such suffixes. Valid characters in the domain name string include letters, digits, hyphens (-), underscores (_), dots (.), and asterisk (*). The asterisk (*) character is used to match a series of domain names with fixed starting or ending string. For example, **www.test.*** includes all domain names starting with **www.test.**; ***.test.gov** includes all domain names ending with **.test.gov**.

New feature: Support for proxy NTLM authentication packets and obtaining the suffix of a Web cache file from the PMO website URL

Configuring extended Web caching features

Enabling Web caching for files in QueryString of a URL

About this task

By default, Web caching does not cache files in QueryString of a URL. After you configure this feature, Web caching can cache the files and it determines whether to cache the files according to other file filtering rules.

Procedure

1. Enter system view.

system-view

2. Enter Web cache view.

Centralized devices:

web-cache

Distributed devices in standalone mode: Centralized IRF devices:

web-cache slot *slot-number*

Distributed devices in IRF mode:

web-cache chassis *chassis-number* **slot** *slot-number*

3. Enable Web caching to cache files in QueryString of a URL.

querystring-file-cache enable

By default, Web caching does not cache files in QueryString of a URL.

Configuring Web caching to ignore the specified HTTP/HTTPS response headers

About this task

The HTTP/HTTPS response header type affects Web caching as follows:

- If the HTTP/HTTPS response has a Cache-Control header, whether Web caching caches the requested Web resources depends on the instructions in the header.
- If the HTTP/HTTPS response has a Set-Cookie header, Web caching does not cache the requested Web resources.
- If the HTTP/HTTPS response has a Vary header, whether Web caching caches the requested Web resources depends on the value for the Vary field.

To make sure Web caching caches the requested Web resources, configure Web caching to ignore the specified HTTP/HTTPS response headers.

Procedure

1. Enter system view.
system-view
2. Enter Web cache view.
Centralized devices:
web-cache
Distributed devices in standalone mode: Centralized IRF devices:
web-cache slot *slot-number*
Distributed devices in IRF mode:
web-cache chassis *chassis-number* **slot** *slot-number*
3. Configure Web caching to ignore the specified HTTP/HTTPS response headers.
cache-ignore { **cache-control** | **set-cookie** | **vary** } *
By default, whether Web caching caches Web resources is affected by the HTTP/HTTPS response header type.

Command reference

New command: cache-ignore

Use **cache-ignore** to configure Web caching to ignore the specified HTTP/HTTPS response headers.

Use **undo cache-ignore** to restore the default.

Syntax

cache-ignore { **cache-control** | **set-cookie** | **vary** } *
undo cache-ignore [**cache-control** | **set-cookie** | **vary**] *

Default

Whether Web caching caches Web resources is affected by the HTTP/HTTPS response header type.

Views

Web cache view

Predefined user roles

network-admin

Parameters

cache-control: Specifies Cache-Control headers.

set-cookie: Specifies Set-Cookie headers.

vary: Specifies Vary headers.

Usage guidelines

The HTTP/HTTPS response header type affects Web caching as follows:

- If the HTTP/HTTPS response has a Cache-Control header, whether Web caching caches the requested Web resources depends on the instructions in the header.
- If the HTTP/HTTPS response has a Set-Cookie header, Web caching does not cache the requested Web resources.

- If the HTTP/HTTPS response has a Vary header, whether Web caching caches the requested Web resources depends on the value for the Vary field.

To make sure Web caching caches the requested Web resources, configure Web caching to ignore the specified HTTP/HTTPS response headers.

Examples

(Centralized devices.) Configure Web caching to ignore the Cache-Control and Vary response headers.

```
<Sysname> system-view
[Sysname] web-cache
[Sysname-web-cache] cache-ignore cache-control vary
```

(Distributed devices in standalone mode.) (Centralized IRF devices.) On slot 1, configure Web caching to ignore the Cache-Control and Vary response headers.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] cache-ignore cache-control vary
```

New command: querystring-file-cache enable

Use **querystring-file-cache enable** to enable Web caching for files in QueryString of a URL.

Use **undo querystring-file-cache enable** to disable Web caching for files in QueryString of a URL.

Syntax

querystring-file-cache enable

undo querystring-file-cache enable

Default

Web caching does not cache files in QueryString of a URL.

Views

Web cache view

Predefined user roles

network-admin

Usage guidelines

After you execute this command, Web caching can cache files in QueryString of a URL, and it determines whether to cache the files according to other file filtering rules.

Examples

(Centralized devices.) Enable Web caching to cache files in QueryString of a URL.

```
<Sysname> system-view
[Sysname] web-cache
[Sysname-web-cache] querystring-file-cache enable
```

(Distributed devices in standalone mode.) (Centralized IRF devices.) On slot 1, enable Web caching to cache files in QueryString of a URL.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] querystring-file-cache enable
```

Related commands

cached-data

cached-extension-name

cached-file

New feature: Enhancing tunnel maintenance

Command reference

New command: debugging system internal tunnel trace

Use **debugging system internal tunnel trace** to enable trace debugging for tunnel running processes.

Use **undo debugging system internal tunnel trace** to disable trace debugging for tunnel running processes.

Syntax

debugging system internal tunnel trace

undo debugging system internal tunnel trace

Default

Trace debugging is disabled for tunnel running processes.

Views

Probe view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command enables the device to trace the tunnel running processes and save the traced information to the **tunnelMdc1Error.log**, **tunnelMdc1Normal.log**, **tunnel_kerror1trace.log**, and **tunnel_knormal1trace.log** files in the **/var/log** directory. To view contents in the .log files, you must install the Devkit feature package and enter bash in user view.

Modified command: display system internal tunnel data

Use **display system internal tunnel data** to display data for a tunnel interface.

Old syntax

Centralized devices:

display system internal tunnel data [**interface tunnel** *number*] [**cpu** *cpu-number*]

Distributed devices in standalone mode: Centralized IRF devices:

display system internal tunnel data [**interface tunnel** *number*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Distributed devices in IRF mode:

```
display system internal tunnel data [ interface tunnel number ] [ chassis  
chassis-number slot slot-number [ cpu cpu-number ] ]
```

New syntax

Centralized devices:

```
display system internal tunnel data [ kernel ] [ interface tunnel number ] [ cpu  
cpu-number ]
```

Distributed devices in standalone mode:Centralized IRF devices:

```
display system internal tunnel data [ kernel ] [ interface tunnel number ] [ slot  
slot-number [ cpu cpu-number ] ]
```

Distributed devices in IRF mode:

```
display system internal tunnel data [ kernel ] [ interface tunnel number ] [ chassis  
chassis-number slot slot-number [ cpu cpu-number ] ]
```

Views

Probe view

Change description

The **kernel** keyword was added to the command. With this keyword specified, the command displays kernel data. Without this keyword, the command displays data in user mode.

New command: display system internal tunnel kernel global run-info

Use **display system internal tunnel kernel global run-info** to display global running information for tunnels in kernel mode.

Syntax

Centralized devices:

```
display system internal tunnel kernel global run-info
```

Distributed devices in standalone mode:Centralized IRF devices:

```
display system internal tunnel kernel global run-info [ slot slot-number [ cpu  
cpu-number ] ]
```

Distributed devices in IRF mode:

```
display system internal tunnel kernel global run-info [ chassis chassis-number slot  
slot-number [ cpu cpu-number ] ]
```

Views

Probe view

Predefined user roles

network-admin

network-operator

Parameters

slot slot-number: Specifies a card by its slot number. If you do not specify a card, this command displays global running information on the active MPU. (Distributed devices in standalone mode.)

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays global running information on the master device. (Centralized IRF devices.)

chassis chassis-number slot slot-number: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays global running information on the global active MPU. (Distributed devices in IRF mode.)

cpu cpu-number: Specifies a CPU by its number. Support for this option depends on the device model.

New command: display system internal tunnel statistics

Use **display system internal tunnel statistics** to display tunnel statistics in kernel or user mode.

Syntax

Centralized devices:

display system internal tunnel [kernel] statistics

Distributed devices in standalone mode: Centralized IRF devices:

display system internal tunnel [kernel] statistics [slot slot-number [cpu cpu-number]]

Distributed devices in IRF mode:

display system internal tunnel [kernel] statistics [chassis chassis-number slot slot-number [cpu cpu-number]]

Views

Probe view

Predefined user roles

network-admin

network-operator

Parameters

kernel: Displays tunnel statistics in kernel mode. If you do not specify this keyword, the command displays tunnel statistics in user mode.

slot slot-number: Specifies a card by its slot number. If you do not specify a card, the command displays tunnel statistics on all cards. (Distributed devices in standalone mode.)

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command displays tunnel statistics on all IRF member devices. (Centralized IRF devices.)

chassis chassis-number slot slot-number: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, the command displays tunnel statistics on all cards. (Distributed devices in IRF mode.)

cpu cpu-number: Specifies a CPU by its number. Support for this option depends on the device model.

New command: display system internal tunnel table

Use **display system internal tunnel table** to display tunnel entries.

Syntax

Centralized devices:

```
display system internal tunnel table type { evi | overlay | overlay6 | uptunnel | uptunnel6 }
```

Distributed devices in standalone mode: Centralized IRF devices:

```
display system internal tunnel table type { evi | overlay | overlay6 | uptunnel | uptunnel6 } [ slot slot-number [ cpu cpu-number ] ]
```

Distributed devices in IRF mode:

```
display system internal tunnel table type { evi | overlay | overlay6 | uptunnel | uptunnel6 } [ chassis chassis-number slot slot-number [ cpu cpu-number ] ]
```

Views

Probe view

Predefined user roles

network-admin

network-operator

Parameters

type: Specifies a tunnel mode.

evi: Specifies EVI tunnel entries.

overlay: Specifies IPv4 VXLAN tunnel entries.

overlay6: Specifies IPv6 VXLAN tunnel entries.

uptunnel: Specifies entries for IPv4 tunnels in up state.

uptunnel6: Specifies entries for IPv6 tunnels in up state.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays tunnel entries on the active MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays tunnel entries on the master device. (Centralized IRF devices.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays tunnel entries on the global active MPU. (Distributed devices in IRF mode.)

cpu *cpu-number*: Specifies a CPU by its number. Support for this option depends on the device model.

New command: display system internal tunnel wait-list

Use **display system internal tunnel wait-list** to display wait-list information for tunnel interfaces.

Syntax

```
display system internal tunnel wait-list
```

Views

Probe view

Predefined user roles

network-admin
network-operator

New command: reset system internal tunnel statistics

Use **reset system internal tunnel statistics** to clear tunnel statistics.

Syntax

Centralized devices:

reset system internal tunnel [**kernel**] **statistics**

Distributed devices in standalone mode: Centralized IRF devices:

reset system internal tunnel [**kernel**] **statistics** [**slot** *slot-number* [**cpu** *cpu-number*]]

Distributed devices in IRF mode:

reset system internal tunnel [**kernel**] **statistics** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

Views

Probe view

Predefined user roles

network-admin
network-operator

Parameters

kernel: Clears tunnel statistics in kernel mode. If you do not specify this keyword, the command clears tunnel statistics in user mode.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, the command clears tunnel statistics on all cards. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command clears tunnel statistics on all IRF member devices. (Centralized IRF devices.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, the command clears tunnel statistics on all cards. (Distributed devices in IRF mode.)

cpu *cpu-number*: Specifies a CPU by its number. Support for this option depends on the device model.

Modified command: debugging tunnel

Use **debugging tunnel** to enable debugging for the tunnel module.

Use **undo debugging tunnel** to disable debugging for the tunnel module.

Old syntax

debugging tunnel { **all** | **error** | **event** | **packet** } [**interface tunnel** *interface-number*]

undo debugging tunnel { **all** | **error** | **event** | **packet** }

New syntax

Centralized devices:

```
debugging tunnel { all | error | event | packet [ acl acl-number ] } [ interface tunnel  
interface-number ]
```

```
undo debugging tunnel { all | error | event | packet }
```

Distributed devices in standalone mode:Centralized IRF devices:

```
debugging tunnel { all | error | event | packet [ acl acl-number ] } [ interface tunnel  
interface-number ] [ slot slot-number ]
```

```
undo debugging tunnel { all | error | event | packet } [ slot slot-number ]
```

Distributed devices in IRF mode:

```
debugging tunnel { all | error | event | packet [ acl acl-number ] } [ interface tunnel  
interface-number ] [ chassis chassis-number slot slot-number ]
```

```
undo debugging tunnel { all | error | event | packet } [ chassis chassis-number slot  
slot-number ]
```

Views

User view

Change description

The following parameters were added:

interface-number: Specifies a tunnel interface by its interface number. If you do not specify a tunnel interface, the command enables tunnel debugging on all interfaces.

acl *acl-number*: : Specifies a basic ACL or an advanced ACL by its number, which is in the range of 2000 to 3999.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, the command enables tunnel debugging on all cards. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command enables tunnel debugging on all IRF member devices. (Centralized IRF devices.) (IRF 3 incapable.)

slot *slot-number*: Specifies an IRF member device by its member ID or specifies a PEX by its virtual slot number. On an IRF fabric, this command enables tunnel debugging on all member devices if you do not specify a member device. On an IRF 3 system, this command enables tunnel debugging on all IRF member devices and PEXs if you do not specify an IRF member device or PEX.(Centralized IRF devices.) (IRF 3 capable.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, the command enables tunnel debugging on all cards. (Distributed devices in IRF mode.) (IRF 3 incapable.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device or specifies a PEX. The *chassis-number* argument represents the member ID of the IRF member device or the virtual chassis number of the PEX. The *slot-number* argument represents the slot number of the card or PEX. On an IRF fabric, this command enables tunnel debugging on all cards if you do not specify a card. On an IRF 3 system, this command enables tunnel debugging on all cards and PEXs if you do not specify a card or PEX. (Distributed devices in IRF mode.) (IRF 3 capable.)

New feature: Configuring dual-device backup for Web caching

Configuring Web caching backup

Web caching backup

The Web cache backup feature enhances the high availability of the Web caching service. You can specify a primary slot and a backup slot for Web caching. When the primary slot fails, the backup slot will take over to provide the Web caching service to ensure service continuity. When the primary slot recovers, the Web caching service switches back to the primary slot.

You can also specify a primary Web caching directory and a backup Web caching directory, which are used by the primary and backup slots to provide the Web caching service, respectively.

Configuring Web caching backup

Restrictions and guidelines

Make sure the storage medium where the Web cache directory resides has sufficient storage space. The Web caching feature saves its operation data and the Web content to be cached to files in the directory. The directory typically needs a storage space of over 1 GB.

The backup Web cache directory for a Web cache view must reside on the backup slot.

Before specifying a Web cache directory, make sure all files in the upper-level directory are using a different name than the Web cache directory or have a file extension.

Procedure

1. Enter system view.
system-view
2. Enter Web cache view.
Centralized devices:
web-cache
Distributed devices in standalone mode:Centralized IRF devices:
web-cache slot *slot-number*
Distributed devices in IRF mode:
web-cache chassis *chassis-number* slot *slot-number*
3. Specify a backup Web caching slot.
Distributed devices in standalone mode:Centralized IRF devices:
backup slot *slot-number*
Distributed devices in IRF mode:
backup chassis *chassis-number* slot *slot-number*
By default, the backup Web caching slot is not set.
4. Set the backup Web cache directory.
file-directory *directory*
By default, the backup Web cache directory is not set.

After the backup Web cache directory is created, the device will not synchronize cache files under the primary directory to the backup directory.

Command reference

New command: dual-gateway-channel

Use **dual-gateway-channel** to configure a channel for traffic direction with the peer gateway.

Use **undo dual-gateway-channel** to delete the traffic direction channels.

Syntax

dual-gateway-channel [**vpn-instance** *vpn-instance-name*] **interface** *interface-type*
interface-number **peer** *ipv4-address*

undo dual-gateway-channel [**vpn-instance** *vpn-instance-name*]

Default

No channels are configured for traffic direction with the peer gateway.

Views

Web cache view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies the VPN instance of the peer gateway. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. The specified VPN instance must have existed. If you do not specify a VPN instance, this command applies to the peer gateway device in the public network.

interface *interface-type interface-number*: Specifies the traffic direction channel interface by its type and number.

peer *ipv4-address*: Specifies the IPv4 address of the peer gateway. This address must be a unicast address.

Usage guidelines

This command applies to the Web cache dual gateway scenario. In this scenario, two gateways provide the Web cache service for users simultaneously, and equal cost paths exist on both the uplink and downlink for Web cache. If the uplink and downlink traffic forwarding paths are not the same, the uplink traffic and downlink traffic will be forwarded to different gateways for processing. The downlink traffic therefore cannot be forwarded to the users and the users cannot access the requested Web resources as a result.

To avoid this issue, you can use this command to configure a traffic direction channel with the peer gateway. If the device receives Web cache downlink traffic for a user that it cannot find, the device forwards the downlink traffic to the peer gateway through the specified channel interface, so the peer gateway can provide Web resources for the user correctly.

NOTE:

In the Web cache dual gateway scenario, the uplink traffic refers to the HTTP/HTTPS requests sent from user hosts to Web servers, and the downlink traffic refers to the HTTP/HTTP responses sent from Web servers to user hosts.

Before you execute this command, disable the Web cache feature. After this command is executed again, enable the Web cache feature again.

Make sure the specified IPv4 address of the peer gateway is reachable, and in the routing table, the outgoing interface for this IPv4 address is the channel interface specified in this command.

You can configure multiple traffic direction channels in multiple VPN instances. If you execute this command for the same VPN instance or for the public network multiple times, the most recent configuration takes effect.

Examples

(Centralized devices.) Specify channel interface GigabitEthernet 1/0/1 for traffic direction with peer gateway 1.1.1.1 in VPN instance **test**.

```
<Sysname> system
[Sysname] web-cache
[Sysname-web-cache] dual-gateway-channel vpn-instance test interface gigabitethernet
1/0/1 peer 1.1.1.1
```

(Distributed devices in standalone mode.) (Centralized IRF devices.) Specify channel interface GigabitEthernet 1/0/1 for traffic direction with peer gateway 1.1.1.1 in VPN instance **test**.

```
<Sysname> system
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] dual-gateway-channel vpn-instance test interface
gigabitethernet 1/0/1 peer 1.1.1.1
```

(Distributed devices in IRF mode.) Specify channel interface GigabitEthernet 1/0/1 for traffic direction with peer gateway 1.1.1.1 in VPN instance **test**.

```
<Sysname> system
[Sysname] web-cache chassis 1 slot 1
[Sysname-web-cache-chassis1-slot1] dual-gateway-channel vpn-instance test interface
gigabitethernet 1/0/1 peer 1.1.1.1
```

New feature: Enabling HTTPS-based Web caching

Enabling HTTPS-based Web caching

Specify listening port numbers

- Specify HTTP listening port numbers.
listen-port *port-number*
- Specify HTTPS listening port numbers.
https listen-port *port-number*

By default, Web caching listens to port 80 for HTTP packets and port 443 for HTTPS packets.

Make sure the specified TCP port number is not being used by any other services on the device. To display TCP port numbers in use, execute the **display tcp verbose** command.

Command reference

New command: https enable

Use **https enable** to enable HTTPS-based Web caching.

Use **undo https enable** to disable HTTP-based Web caching.

Syntax

https enable

undo https enable

Default

HTTPS-based Web caching is disabled.

Views

Web cache view

Predefined user roles

network-admin

Usage guidelines

Before enabling HTTPS-based Web caching, you must configure the types of the webpage files to be cached and the Web cache directory.

When the device enabled with HTTPS-based Web caching attempts to cache Web resources accessed by a user through HTTPS, the user will be prompted with a certificate warning. Because the certificate of the device is a private CA-issued digital certificate, it cannot pass the verification of the user host. To resolve this issue, the user can export the device's CA root certificate file (webcache_cacert.crt) from the Web caching working directory and import it to the trusted certificate authorities store. Then, the device' certificate can pass the verification of the user host so the user will not be prompted with the certificate warning.

Examples

(Centralized devices.) Enable HTTPS-based Web caching.

```
<Sysname> system-view
```

```
[Sysname] web-cache
```

```
[Sysname-web-cache] https enable
```

(Distributed devices in standalone mode.) Enable HTTPS-based Web caching.

```
<Sysname> system-view
```

```
[Sysname] web-cache slot 1
```

```
[Sysname-web-cache-slot1] https enable
```

(Distributed devices in IRF mode.) Enable HTTPS-based Web caching.

```
<Sysname> system-view
```

```
[Sysname] web-cache chassis 1 slot 1
```

```
[Sysname-web-cache-chassis1-slot1] https enable
```

Related commands

file-directory

cached-data

New command: https listen-port

Use **https listen-port** to set a port number for Web caching to listen for HTTPS packets.

Use **undo https listen-port** to remove listening port numbers specified for Web caching to listen for HTTPS packets.

Syntax

https listen-port *port-number*

undo https listen-port

Default

Web caching listens to port 443 for HTTPS packets.

Views

Web cache view

Predefined user roles

network-admin

Parameters

port-number: Specifies a TCP port number for Web caching to listen for HTTPS packets (HTTPS listening port number for Web caching). The value range is 1 to 65535.

Usage guidelines

Make sure the specified TCP port number is not being used by any other services on the device. To display TCP port numbers in use, execute the **display tcp verbose** command.

Before changing the listening port setting, you must disable HTTPS-based Web caching. After changing the listening port setting, enable HTTPS-based Web caching again.

Examples

(Centralized devices.) Set the port number to 655 for Web caching to listen for HTTPS packets.

```
<Sysname> system-view
[Sysname] web-cache
[Sysname-web-cache] https listen-port 655
```

(Distributed devices in standalone mode.) Set the port number to 655 for Web caching to listen for HTTPS packets.

```
<Sysname> system-view
[Sysname] web-cache slot 1
[Sysname-web-cache-slot1] https listen-port 655
```

(Distributed devices in IRF mode.) Set the port number to 655 for Web caching to listen for HTTPS packets.

```
<Sysname> system-view
[Sysname] web-cache chassis 1 slot 1
[Sysname-web-cache-chassis1-slot1] https listen-port 655
```

Related commands

https enable

Modified command: listen-port

Use **listen-port** to set a port number for Web caching to listen for HTTP packets.

Use **undo listen-port** to remove listening port numbers specified for Web caching to listen for HTTP packets.

Syntax

listen-port *port-number*

undo listen-port

Views

Web cache view

Change description

- The command description is changed.
 - Before modification: Use **listen-port** to specify the Web caching listening port number.
 - After modification: Use **listen-port** to set a port number for Web caching to listen for HTTP packets.
- The default setting is changed.
 - Before modification: Web caching listens to port 80.
 - After modification: Web caching listens to port 80 for HTTP packets.
- The parameter description is changed.
 - Before modification: The *port-number* argument specifies a TCP port number in the range of 1 to 65535.
 - After modification: The *port-number* argument specifies a TCP port number for Web caching to listen for HTTP packets (HTTP listening port number for Web caching). The value range is 1 to 65535.
- The usage guidelines are changed.
 - Before modification:

Make sure the specified TCP port number is not being used by any other services on the device. To display TCP port numbers in use, execute the **display tcp verbose** command.

If you do not configure this command, the device does not listen to any port. As a best practice, execute this command before you enable Web caching.

Before changing the listening port setting, you must disable Web caching. After changing the listening port setting, enable Web caching again.
 - After modification:

Make sure the specified TCP port number is not being used by any other services on the device. To display TCP port numbers in use, execute the **display tcp verbose** command.

Before changing the listening port setting, you must disable Web caching. After changing the listening port setting, enable Web caching again.

New feature: ADVPN support specifying the link protocol type of the hub

Configuring hub groups

About this task

Hub groups apply to large ADVPN networks. You can classify spokes to different hub groups, and specify one or more hubs for each group. The VAM server assigns a client only the hub information

of the client's own hub group. A client establishes permanent ADVPN tunnels only to the hubs in its own hub group.

By default, spokes are not allowed to establish direct tunnels. If an ACL is specified to control establishing spoke-spoke tunnels, the VAM server assigns the specified ACL to an online hub. The hub uses the ACL to match received packets. If a match is found, the hub sends a redirect packet to the spoke that sent the packet. Then, the spoke sends the VAM server the destination address of the packet, obtains the remote spoke information, and establishes a direct tunnel to the remote spoke.

After a spoke-spoke tunnel is established, the spokes directly exchange packets.

When a VAM client registers with the VAM server, the VAM server selects a hub group for the client as follows:

1. The server matches the private address of the client against the private addresses of hubs in different hub groups in lexicographic order.
2. If a match is found, the server assigns the client to the hub group as a hub.
3. If no match is found, the server matches the client's private address against the private addresses of spokes in different hub groups in lexicographic order.
4. If a match is found, the server assigns the client to the hub group as a spoke.
5. If no match is found, the registration fails.

Procedure

1. Enter system view.

system-view

2. Enter ADVPN domain view.

vam server advpn-domain *domain-name* [**id** *domain-id*]

3. Create a hub group and enter hub group view.

hub-group *group-name*

4. Configure a hub private address.

IPv4:

hub private-address *private-ip-address* [**advpn-port** *port-number* | **public-address** { *public-ipv4-address* | *public-ipv6-address* } [**advpn-port** *port-number*] [**link-protocol** { **gre** | **ipsec-gre** | **ipsec-udp** [**registered-address** { *registered-ipv4-address* | *registered-ipv6-address* } [**registered-advpn-port** *port-number*]] | **udp** }]]

IPv6:

hub ipv6 private-address *private-ipv6-address* [**advpn-port** *port-number* | **public-address** { *public-ipv4-address* | *public-ipv6-address* } [**advpn-port** *port-number*] [**link-protocol** { **gre** | **ipsec-gre** | **ipsec-udp** [**registered-address** { *registered-ipv4-address* | *registered-ipv6-address* } [**registered-advpn-port** *port-number*]] | **udp** } **link-local-address** *link-local-address*]]

By default, no hub private addresses are configured.

A hub group must have a minimum of one hub private address.

5. Configure a spoke private address range.

IPv4:

spoke private-address { **network** *ip-address* { *mask-length* | *mask* } | **range** *start-ipv4-address* *end-ipv4-address* }

IPv6:

spoke ipv6 private-address { **network** *prefix* *prefix-length* | **range** *start-ipv6-address* *end-ipv6-address* }

By default, no spoke private address ranges are configured.

You can configure multiple spoke private IPv4 and IPv6 address ranges in a hub group.

6. Specify an ACL to control establishing spoke-to-spoke tunnels.

IPv4:

shortcut interest { **acl** { *acl-number* | **name** *acl-name* } **all** }

IPv6:

shortcut ipv6 interest { **acl** { *ipv6-acl-number* | **name** *ipv6-acl-name* } | **all** }

By default, spokes are not allowed to establish direct tunnels.

Command reference

Modified command: hub ipv6 private-address

Use **hub ipv6 private-address** to configure a hub private IPv6 address in a hub group.

Use **undo hub ipv6 private-address** to remove a hub private IPv6 address from a hub group.

Old syntax

hub ipv6 private-address *private-ipv6-address* [**public-address** { *public-ip-address* | *public-ipv6-address* } [**advpn-port** *port-number*]]

undo hub ipv6 private-address *private-ipv6-address*

New syntax

hub ipv6 private-address *private-ipv6-address* [**advpn-port** *port-number* | **public-address** { *public-ipv4-address* | *public-ipv6-address* } [**advpn-port** *port-number*] [**link-protocol** { **gre** | **ipsec-gre** | **ipsec-udp** [**registered-address** { *registered-ipv4-address* | *registered-ipv6-address* } [**registered-advpn-port** *port-number*]] | **udp** } **link-local-address** *link-local-address*]]

undo hub ipv6 private-address *private-ipv6-address*

Views

Hub group view

Parameters

The *public-ip-address* argument was changed to the *public-ipv4-address* argument.

The following parameters were added:

link-protocol: Specifies the link protocol of the hub.

gre: Specifies GRE.

ipsec-gre: Specifies IPsec-protected GRE.

ipsec-udp: Specifies IPsec-protected UDP.

udp: Specifies UDP.

registered-address: Specifies the registered public address of the hub (public address before NAT). Configure this parameter only when the link protocol of the hub is IPsec-protected UDP and the hub is behind a NAT gateway.

registered-ipv4-address: Specifies the registered IPv4 public address of the hub. The address must be a unicast address.

registered-ipv6-address: Specifies the registered IPv6 public address of the hub. The address must be a global unicast address.

registered-advpn-port *port-number*: Specifies the registered ADVPN port number of the hub (ADVPN port number before NAT). If you do not specify an ADVPN port number, the default ADVPN port number 18001 is used.

link-local-address *link-local-address*: Specifies the IPv6 link-local address of the hub to ensure IPv6 network connectivity.

Usage guidelines

Before modification

Typically, you do not need to the public address and ADVPN port number of a hub. For a hub to traverse a NAT gateway, configure a static mapping between the hub's registered public address/ADVPN port number and a NATed address/port number on the NAT gateway. To use this command to add the hub to a hub group, specify the NATed address and port number as the public address and ADVPN port number.

After modification

Typically, you only need to specify the private address of a hub. Other parameters are optional. However, you must specify other parameters in addition to the private address of the hub in the following scenarios:

- **Hub information can be automatically obtained and the hub is behind a NAT gateway**—For the hub to traverse the NAT gateway, a static mapping between the hub's registered public address/ADVPN port number and a NATed address/port number must be configured on the NAT gateway. To execute this command for the hub, specify the NATed address and port number as the public address and ADVPN port number in the command.
- **Hub information is manually configured and the hub is not behind a NAT gateway**—To ensure that a spoke can come online before the hub comes online after the VAM server reboots, use this command to manually configure hub information on the VAM server. The information includes the public address, ADVPN port number, link protocol, and IPv6 link-local address of the hub. The spoke can obtain the manually configured hub information from the VAM server to establish an ADVPN tunnel with the hub after the VAM server reboots.
- **Hub information is manually configured and the hub is behind a NAT gateway**—If the link protocol of the hub is IPsec-protected UDP, configure the parameters as follows:
 - Use the **public-address** { *public-ipv4-address* | *public-ipv6-address* } option to specify the NATed address as the public address.
 - Use the **advpn-port** *port-number* option to specify the port number NATed from IPsec port 4500 as the ADVPN port number.
 - Use the **registered-address** { *registered-ipv4-address* | *registered-ipv6-address* } option to specify the public address of the hub before NAT.
 - Use the **registered-advpn-port** *port-number* option to specify the ADVPN port number before NAT.

If the link protocol is UDP, you only need to specify the NATed address and port number configured on the NAT gateway as the public address and ADVPN port number.

If the manually configured hub information is inconsistent with the automatically registered hub information on the VAM server, the automatically registered hub information takes effect.

Modified command: hub private-address

Use **hub private-address** to configure a hub private IPv4 address in a hub group.

Use **undo hub private-address** to remove a hub private IPv4 address from a hub group.

Old syntax

```
hub private-address private-ip-address [ public-address { public-ipv4-address |  
public-ipv6-address } [ advpn-port port-number ] ]  
undo hub private-address private-ip-address
```

New syntax

```
hub private-address private-ip-address [ advpn-port port-number | public-address  
{ public-ipv4-address | public-ipv6-address } [ advpn-port port-number ] [ link-protocol  
{ gre | ipsec-gre | ipsec-udp [ registered-address { registered-ipv4-address |  
registered-ipv6-address } [ registered-advpn-port port-number ] ] | udp } ] ]  
undo hub private-address private-ip-address
```

Views

Hub group view

Parameter changes

The following parameters were added:

link-protocol: Specifies the link protocol of the hub.

gre: Specifies GRE.

ipsec-gre: Specifies IPsec-protected GRE.

ipsec-udp: Specifies IPsec-protected UDP.

udp: Specifies UDP.

registered-address: Specifies the registered public address of the hub (public address before NAT). Configure this parameter only when the link protocol of the hub is IPsec-protected UDP and the hub is behind a NAT gateway.

registered-ipv4-address: Specifies the registered IPv4 public address of the hub. The address must be a unicast address.

registered-ipv6-address: Specifies the registered IPv6 public address of the hub. The address must be a global unicast address.

registered-advpn-port port-number: Specifies the registered ADVPN port number of the hub (ADVPN port number before NAT). If you do not specify an ADVPN port number, the default ADVPN port number 18001 is used.

Usage guidelines

Before modification

For a hub to traverse a NAT gateway, configure a static mapping between the hub's registered public address/ADVPN port number and a NATed address/port number on the NAT gateway. To use this command to add the hub to a hub group, specify the NATed address and port number as the public address and ADVPN port number.

After modification

Typically, you only need to specify the private address of a hub. Other parameters are optional. However, you must specify other parameters in addition to the private address of the hub in the following scenarios:

- **Hub information can be automatically obtained and the hub is behind a NAT gateway**—For the hub to traverse the NAT gateway, a static mapping between the hub's registered public address/ADVPN port number and a NATed address/port number must be configured on the NAT gateway. To execute this

command for the hub, specify the NATed address and port number as the public address and ADVPN port number in the command.

- **Hub information is manually configured and the hub is not behind a NAT gateway**—To ensure that a spoke can come online before the hub comes online after the VAM server reboots, use this command to manually configure hub information on the VAM server. The information includes the public address, ADVPN port number, link protocol, and IPv6 link-local address of the hub. The spoke can obtain the manually configured hub information from the VAM server to establish an ADVPN tunnel with the hub after the VAM server reboots.
- **Hub information is manually configured and the hub is behind a NAT gateway**—If the link protocol of the hub is IPsec-protected UDP, configure the parameters as follows:
 - Use the **public-address** { *public-ipv4-address* | *public-ipv6-address* } option to specify the NATed address as the public address.
 - Use the **advpn-port** *port-number* option to specify the port number NATed from IPsec port 4500 as the ADVPN port number.
 - Use the **registered-address** { *registered-ipv4-address* | *registered-ipv6-address* } option to specify the public address of the hub before NAT.
 - Use the **registered-advpn-port** *port-number* option to specify the ADVPN port number before NAT.

If the link protocol is UDP, you only need to specify the NATed address and port number configured on the NAT gateway as the public address and ADVPN port number.

If the manually configured hub information is inconsistent with the automatically registered hub information on the VAM server, the automatically registered hub information takes effect.

New feature: GRE keepalive support for the reply-check-only mode

Configuring a GRE/IPv4 tunnel

Restrictions and guidelines

This task describes only GRE/IPv4 tunnel required tunnel interface commands (the **interface tunnel**, **source**, **destination** and **tunnel dfbit enable** commands). For more tunnel interface commands, see tunneling configuration in *Layer 3—IP Services Configuration Guide*.

Do not use the **gre key** and **gre vpc enable** commands on the same tunnel interface.

Procedure

1. Enter system view.

system-view

2. Create a GRE tunnel interface, and specify the tunnel mode as GRE/IPv4.

interface tunnel *number* **mode gre**

You must configure the same tunnel mode on both ends of a tunnel. Otherwise, packet delivery might fail.

3. Configure an IP address for the tunnel interface based on the passenger protocol.

IPv4:

For information about how to assign an IPv4 address to an interface, see IP addressing configuration in *Layer 3—IP Services Configuration Guide*.

IPv6:

For information about how to assign an IPv6 address to an interface, see IPv6 basics configuration in *Layer 3—IP Services Configuration Guide*.

By default, no IP address is configured for a tunnel interface.

4. Configure a source address or source interface for the tunnel.

source { *ip-address* | *interface-type interface-number* }

By default, no source address or interface is configured for a tunnel.

If you configure a source address, the tunnel interface uses the source address as the source address of encapsulated packets.

If you configure a source interface, the tunnel interface uses the primary IP address of the source interface as the source address of encapsulated packets.

5. Configure a destination address for the tunnel.

destination *ip-address*

By default, no destination address is configured for a tunnel.

The destination address is the address of the physical interface that the tunnel remote end uses to receive packets from the GRE tunnel.

The tunnel local end uses this address as the destination address of encapsulated packets.

The tunnel destination address and the IP address of the tunnel interface must be in different subnets.

6. (Optional.) Enable GRE keepalive, set the keepalive interval and keepalive number, and configure the keepalive mode.

keepalive [**reply-check-only**] [*interval* [*times*]]

By default, GRE keepalive is disabled.

7. (Optional.) Configure GRE security mechanisms.

- o Enable GRE checksum.

gre checksum

By default, GRE checksum is disabled.

- o Configure a GRE key for the GRE tunnel interface.

gre key *key*

By default, no GRE key is configured for a GRE tunnel interface.

The two ends of a GRE tunnel must have the same key or both have no key.

8. (Optional.) Set the DF bit for encapsulated packets.

tunnel dfbit enable

By default, the DF bit is not set, allowing encapsulated packets to be fragmented.

9. (Optional.) Enable GRE packets to carry VPC information.

gre vpc enable

By default, GRE packets do not carry VPC information.

10. (Optional.) Specify a service class value for the GRE tunnel interface.

service-class *service-class-value*

By default, no service class value is specified for a GRE tunnel interface.

Command reference

Modified command: keepalive

Use **keepalive** to enable GRE keepalive and EoGRE and set the keepalive interval and the keepalive number, and configure the keepalive mode.

Use **undo keepalive** to disable and EoGRE GRE keepalive.

Old syntax

keepalive [*interval* [*times*]]

undo keepalive

Old syntax

keepalive [**reply-check-only**] [*interval* [*times*]]

undo keepalive

Views

Tunnel interface view

Change description

The **reply-check-only** keyword was added.

reply-check-only: Enables the reply-check-only keepalive mode. In this mode, the device places the tunnel interface state to up only when it receives a keepalive acknowledgment packet replied from the peer. The reply-check-only mode is disabled by default. If you do not specify this keyword, the device places the tunnel interface state to up when it receives a keepalive packet initiated or replied from the peer.

Enable the reply-check-only mode in scenarios where the local device can receive keepalive packets from the peer but cannot send keepalive packets, such as remote-to-local one-way communication of a tunnel. In such a scenario, the peer shuts down the tunnel interface because it cannot receive keepalive packets from the local device. The local device, however, brings up the tunnel interface mistakenly when it receives a keepalive probe packet initiatively sent from the peer. After the reply-check-only mode is enabled, the local device brings up the tunnel interface only when it receives a keepalive probe reply from the peer. It keeps the tunnel interface down when it receives keepalive probe packets from the peer, so as to avoid setting wrong tunnel interface state.

Modified command: display interface tunnel

Use **display interface tunnel** to display tunnel interface information.

Syntax

display interface [**tunnel** [*number*]] [**brief** [**description** | **down**]]

Views

Any view

Change description

The following fields were added or edited in the command output:

Field	Description
Tunnel keepalive enabled, replay-check-only, Period(xx s),	GRE keepalive is enabled for the tunnel interface and the keepalive mode is checking only keepalive reply packets. The keepalive

Retries(x)	interval is xx seconds and the maximum number of keepalive retries is x. This field is not displayed if the keepalive reply-check-only feature is not configured.
Tunnel keepalive disabled	GRE keepalive is disabled. This field is not displayed if the keepalive feature is enabled.
Checksumming of GRE packets disabled	The GRE packet checksum feature is disabled.
Checksumming of GRE packets enabled	The GRE packet checksum feature is enabled.

New feature: eMDI

About eMDI

Enhanced Media Delivery Index (eMDI) is a solution to audio and video service quality monitoring and fault locating. It is intended to solve problems caused by packet loss, packet sequence errors, and jitters.

eMDI monitors and analyzes specific TCP or RTP packets on each node of an IP network in real time, providing data for you to quickly locate network faults.

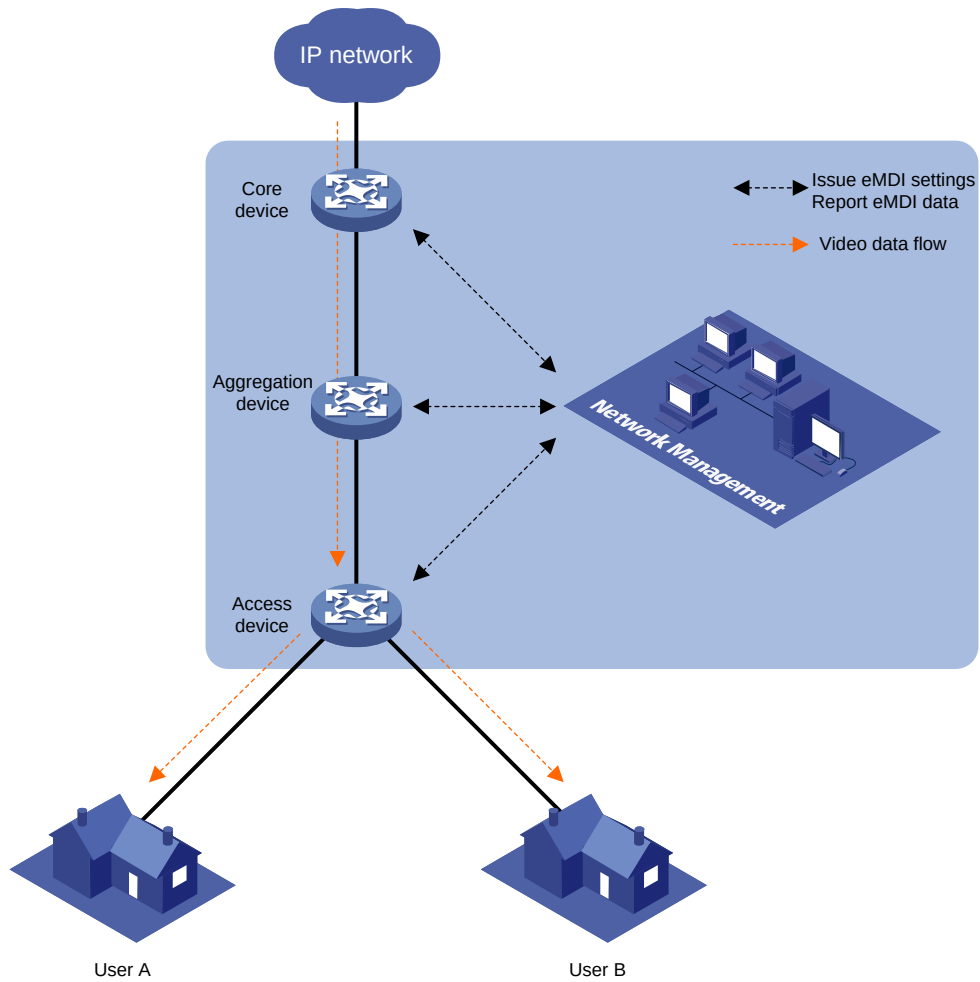
eMDI implementation

The eMDI feature is implemented on the basis of eMDI instances. Each eMDI instance monitors one data flow as defined by its parameters. It inspects fields of packets, periodically collects statistics, and reports to the NMS.

Figure 45 shows the eMDI deployment and operating process.

1. Upon service quality deterioration, you can obtain the data flow characteristics from the headers of interested packets, such as the source and destination IP addresses.
2. You deploy eMDI on each device that the data flow traverses by using the NMS or CLI.
3. The devices monitor the data flows, collect statistics, and report monitoring data to the NMS.
4. The NMS collects and analyzes the monitoring data and displays the analysis results graphically.
5. Based on the analysis results, you can quickly locate the network faults.

Figure 45 eMDI network diagram



Monitored items

Table 83 and Table 84 list the monitored items for TCP packets and UDP packets. RTP packets are carried in UDP packets.

Table 83 Monitored items for TCP packets

Item	Description	Calculation formula	Remarks
Rate	Packet input rate, in bps or pps.	- Rate (bps) = Total length of packets received within a monitoring period / Monitoring period - Rate (pps) = Number of packets received within a monitoring period / Monitoring period	This item is intended for unidirectional flows.
UPLR	Upstream packet loss rate, in units of one hundred thousandth.	$UPLR = (\text{Number of lost upstream packets} / (\text{Number of received packets} + \text{Number of lost upstream packets})) / 100000$	If no packets are lost, the sequence number of the current packet plus the length of the current packet is the expected sequence number of the next packet. If the

Item	Description	Calculation formula	Remarks
			sequence number of the next packet is greater than the expected sequence number, packet loss has occurred on an upstream device. The number of lost packets can be calculated based on the average packet size. This item is intended for unidirectional flows.
DPLR	Downstream packet loss rate, in units of one hundred thousandth.	- Number of lost downstream packets = Total number of lost packets – Number of lost upstream packets $DPLR = (\text{Number of lost downstream packets} / \text{Number of received packets}) / 100000$	If no packets are lost, the sequence number of the current packet plus the length of the current packet is the expected sequence number of the next packet. If the sequence number of the next packet is smaller than the expected sequence number, the packet is considered to be a retransmitted packet. The number of retransmitted packets is considered to be the total number of lost packets. This item is intended for unidirectional flows.
DRTT	Average downstream round trip time, in microseconds.	$DRTT = T2 - T1$	The timestamp for a received non-retransmitted packet is recorded as T1. The sequence number of the packet plus the length of the packet is the expected sequence number of the next packet. If the sequence number of an ACK packet received from a downstream device is greater than or equal to the expected number, the timestamp of the ACK packet is recorded as T2. DRTT is equal to the average value of the differences between the T2 values and the corresponding T1 values. This item is intended for bidirectional flows.
URTT	Average upstream round trip time, in microseconds.	$URTT = T2 - T1$	T1 indicates the timestamp when the device finds a SYN packet sent by the client for a connection. T2 indicates the timestamp when the device finds a SYN ACK packet returned by the server. Because URTT calculation depends on TCP control

Item	Description	Calculation formula	Remarks
			packets, it might not be calculated within a monitoring period. This item is intended for bidirectional flows.

Table 84 Monitored items for UDP packets

Item	Description	Calculation formula	Remarks
RTP-LR	RTP packet loss rate, in units of one hundred thousandth.	$\text{RTP-LR} = (\text{Number of lost packets} / (\text{Number of received packets} + \text{Number of lost packets} - \text{Number of out-of-order packets})) / 100000$	If the difference between the sequence number of current RTP packet and the greatest sequence number of earlier RTP packets is greater than 1, packet loss has occurred. If the sequence number of the current RTP packet is smaller than the sequence numbers of all earlier RTP packets, the packet is an out-of-order packet. This item is intended for unidirectional flows.
RTP-SER	RTP packet sequence error rate, in units of one hundred thousandth.	$\text{RTP-SER} = (\text{Number of out-of-order packets} / (\text{Number of received packets} + \text{Number of lost packets} - \text{Number of out-of-order packets})) / 100000$	This item is intended for unidirectional flows.
Jitter	RTP packet jitter, in microseconds.	$\text{Jitter} = T2 - T1$	T1 represents the interval between the time when the sender sends the first packet and the time when the sender sends the last packet. T2 represents the interval between the time when the receiver receives the first packet and the time when the receiver receives the last packet. This item is intended for unidirectional flows.
RTP-LP	Maximum number of continuously lost RTP packets.	The RTP-LP value uses the maximum number of continuously lost RTP packets within a monitoring period.	On a service provider network with the retransmission threshold set, you can compare the RTP-LP value with the retransmission threshold to identify the existence of faults. The retransmission mechanism can address loss of a small number of packets. The greater the RTP-LP value is, the less the retransmission mechanism can help. This item is intended for

Item	Description	Calculation formula	Remarks
			unidirectional flows.
RTP-ELF	RTP effective loss factor for Forward Error Correct (FEC), in units of one hundred thousandth.	The RTP-ELF value is calculated based on the FEC sliding window and packet loss threshold. After each window slide, the system identifies whether the number of lost data packets in the window within the monitoring period is greater than the threshold. If yes, the system increases RTP-ELF by 1. The window sliding stops when the monitoring period expires.	If the total number of packet loss windows is greater than 0 within a monitoring period, a video fault exists.

Restrictions: Hardware compatibility with eMDI

The RSE-X3 MPUs do not support eMDI.

The following matrixes show support of hardware platforms for eMDI:

Hardware	eMDI compatibility
MSR610	No
MSR 810, MSR 810-W, MSR 810-W-DB, MSR 810-LM, MSR 810-W-LM, MSR 810-10-PoE, MSR 810-LM-HK, MSR 810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR 810-LMS, MSR 810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR 2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR 2630	No
MSR 3600-28, MSR 3600-51	No
MSR 3600-28-SI, MSR 3600-51-SI	No
MSR 3600-28-X1, MSR 3600-28-X1-DP, MSR 3600-51-X1, MSR 3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	Yes
MSR 3610-I-DP, MSR 3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	Yes
MSR 3610-X1, MSR 3610-X1-DP, MSR 3610-X1-DC, MSR 3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR 3610, MSR 3620, MSR 3620-DP, MSR 3640, MSR 3660	Yes

Hardware	eMDI compatibility
MSR 3610-G, MSR 3620-G	Yes
MSR3640-G	Yes
MSR3640-X1-HI	Yes

Hardware	eMDI compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	Yes

Hardware	eMDI compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	Yes
MSR3610-I-XS	Yes
MSR3610-IE-XS	Yes
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	eMDI compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No

MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Restrictions and guidelines

eMDI is required on each node that monitored data flows traverse.

An eMDI instance can monitor only one data flow. The data flows for different eMDI instances cannot be the same or overlapped.

The following data flows are overlapped:

- **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2**
- **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2 destination-port 20**

The following data flows are not overlapped:

- **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2 destination-port 10**
- **flow ipv4 tcp source 1.1.1.1 destination 2.2.2.2 destination-port 20**

The **clock-rate** keyword for the **flow ipv4 udp** command does not result in UDP flow overlapping.

A started eMDI instance automatically stops upon a master/subordinate or active/standby switchover. You must execute the **start** command again to start the instance.

To modify the configuration for an eMDI instance that is already started, stop the instance first by executing the **stop** command.

Incomplete eMDI data might cause deviations in the monitoring results. The eMDI data is incomplete in the following situations:

- Not all packets of the monitored data flow pass through the device.
- All packets of the monitored data flow pass through the device, but not all of the packets are forwarded by the same module.

Prerequisites

Identify the characteristics of the data flows to be monitored so you can specify data flows for eMDI instances.

Configuring eMDI

Configuring an eMDI instance

1. Enter system view.
system-view
2. Enable eMDI and enter its view.
emdi
By default, eMDI is disabled.
3. (Optional.) Set the maximum number of packets sampled per monitoring period for all eMDI instances.
monitor-period-packet maximum *max-number*
4. Create an eMDI instance and enter its view.

instance *instance-name*

By default, no eMDI instance exists.

5. (Optional.) Configure a description for the eMDI instance.

description *text*

By default, an eMDI instance does not have a description.

6. Specify the data flow to be monitored by using the eMDI instance.

Choose one option as needed:

- Specify a TCP data flow.

flow ipv4 tcp source *source-ip-address* **destination** *destination-ip-address*
[**destination-port** *destination-port-number* | **source-port** *source-port-number* | **vlan**
vlan-id | **vni** *vxlan-id* | **vpn-instance** *vpn-instance-name*] *

- Specify a UDP data flow.

flow ipv4 udp source *source-ip-address* **destination** *destination-ip-address*
[**destination-port** *destination-port-number* | **source-port** *source-port-number* |
vlan *vlan-id* | **vni** *vxlan-id* | **pt** *pt-value* | **clock-rate** *clock-rate-value* | **vpn-instance**
vpn-instance-name] *

By default, no data flow is specified for an eMDI instance.

Specifying more options defines a more granular data flow and provides more helpful monitoring data and analysis results. For example, to monitor the data from 10.0.0.1 to 10.0.1.1/100, specify the destination port number. If you do not specify the destination port number, the instance monitors the flow that the first received matching packet represents, which might cause deviations on the monitoring results.

7. (Optional.) Set the alarm thresholds for the eMDI instance.

alarm { **dplr** | **rtp-lr** | **rtp-ser** | **uplr** } **threshold** *threshold-value*

By default, the alarm thresholds for an eMDI instance are all 100.

A TCP data flow supports only the **dplr** and **uplr** keywords and a UDP data flow supports only the **rtp-lr** and **rtp-ser** keywords.

8. (Optional.) Set the eMDI alarm logging threshold, that is, the number of consecutive alarms to be suppressed before logging the event.

alarm suppression times *times-value*

By default, the eMDI alarm logging threshold is 3.

9. (Optional.) Specify the sliding window size and packet loss threshold for the UDP data flow to be monitored.

fec { **window** *window-size* | **threshold** *threshold-value* } *

By default, the sliding window size and packet loss threshold for the UDP data flow is 100 and 5, respectively.

10. (Optional.) Specify the eMDI instance lifetime.

lifetime { **seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days* }

By default, the eMDI instance lifetime is 1 hour.

11. (Optional.) Specify the monitoring period for the eMDI instance.

monitor-period *period-value*

By default, the monitoring period for an eMDI instance is 60 seconds.

Starting an eMDI instance

1. Enter system view.

- system-view**
- 2. Enter eMDI view.
emdi
- 3. Enter eMDI instance view.
instance *instance-name*
- 4. Start the eMDI instance.
Start

Stopping an eMDI instance

To stop a single eMDI instance:

- 1. Enter system view.
system-view
- 2. Enter eMDI view.
emdi
- 3. Enter eMDI instance view.
instance *instance-name*
- 4. Stop the eMDI instance.
Stop

To stop all eMDI instances:

- 5. Enter system view.
system-view
- 6. Enter eMDI view.
emdi
- 7. Stop all eMDI instances.
stop all

Display and maintenance commands for eMDI

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display eMDI instance information.	display emdi instance [name <i>instance-name</i> id <i>instance-id</i>] [verbose]
Display eMDI instance resource information.	display emdi resource
Display monitoring statistics for an eMDI instance.	display emdi statistics { instance-name <i>instance-name</i> instance-id <i>instance-id</i> } [number <i>number</i>] [abnormal verbose]
Clear eMDI statistics.	reset emdi statistics [instance-name <i>instance-name</i> instance-id <i>instance-id-value</i>]

Command reference

alarm suppression times

Use **alarm suppression times** to set the eMDI alarm logging threshold, that is, the number of consecutive alarms to be suppressed before logging the event.

Use **undo alarm suppression times** to restore the default.

Syntax

alarm suppression times *times-value*

undo alarm suppression times

Default

The eMDI alarm logging threshold is 3.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

times-value: Specifies the number of consecutive alarms to be suppressed before logging the event, in the range of 0 to 60. To disable eMDI alarm logging, set this argument to 0.

Usage guidelines

A started eMDI instance monitors its data flow and periodically collects statistics on lost and out-of-order packets.

- If a statistic is equal to or greater than the alarm threshold, the instance triggers an alarm. When the number of consecutive alarms of the same type exceeds the logging threshold, the device sends an alarm log message to the information center.
- If a statistic is less than the alarm threshold, the instance records an alarm removal event. When the number of consecutive alarm removal events of the same type exceeds the logging threshold, the device sends an alarm-removed log message to the information center.

For more information about the information center, see "Configuring information center."

To change the eMDI alarm logging threshold for an eMDI instance that is already started, you must stop the instance first by executing the **stop** command.

Examples

```
# Set the eMDI alarm logging threshold to 5.
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI1
[Sysname-emdi-instance-eMDI1] flow ipv4 tcp source 10.0.0.1 destination 10.2.2.2
[Sysname-emdi-instance-eMDI1] alarm suppression times 5
```

Related commands

flow ipv4 tcp

flow ipv4 udp

alarm threshold

Use **alarm threshold** to set alarm thresholds for an eMDI instance.

Use **undo alarm threshold** to restore the defaults.

Syntax

```
alarm { dplr | rtp-lr | rtp-ser | uplr } threshold threshold-value  
undo alarm { dplr | rtp-lr | rtp-ser | uplr } threshold
```

Default

The alarm thresholds for an eMDI instance are all 100.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

dplr: Sets the alarm threshold for the downstream TCP packet loss rate.

rtp-lr: Sets the alarm threshold for the RTP packet loss rate.

rtp-ser: Sets the alarm threshold for the RTP packet sequence error rate.

uplr: Sets the alarm threshold for the upstream TCP packet loss rate.

threshold-value: Specifies the alarm threshold value, which is the number of lost or out-of-order packets among 100000 packets. The value range is 1 to 100000.

Usage guidelines

A started eMDI instance monitors its data flow and periodically collects statistics on lost and out-of-order packets.

- If a statistic is equal to or greater than the alarm threshold, the instance triggers an alarm. When the number of consecutive alarms of the same type exceeds the logging threshold, the device sends an alarm log message to the information center.
- If a statistic is less than the alarm threshold, the instance records an alarm removal event. When the number of consecutive alarm removal events of the same type exceeds the logging threshold, the device sends an alarm-removed log message to the information center.

For more information about the information center, see "Configuring information center."

To modify alarm thresholds for an eMDI instance that is already started, you must stop the instance first by executing the **stop** command.

Examples

Set the downstream TCP packet loss rate to 1/100 for eMDI instance **eMDI1**.

```
<Sysname> system-view  
[Sysname] emdi  
[Sysname-emdi] instance eMDI1  
[Sysname-emdi-instance-eMDI1] flow ipv4 tcp source 10.0.0.1 destination 10.2.2.2  
[Sysname-emdi-instance-eMDI1] alarm dplr threshold 1000
```

Related commands

flow ipv4 tcp
flow ipv4 udp

description

Use **description** to configure a description for an eMDI instance.

Use **undo description** to restore the default.

Syntax

description *text*
undo description

Default

An eMDI instance does not have a description.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 255 characters.

Usage guidelines

You can use this command to add, delete, or modify the description for a running instance.

Examples

```
# Set the description to eMDI1 for eMDI instance eMDI1.
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI1
[Sysname-emdi-instance-eMDI1] description eMDI1
```

display emdi instance

Use **display emdi instance** to display eMDI instance information.

Syntax

display emdi instance [**name** *instance-name* | **id** *instance-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

name *instance-name*: Specifies an eMDI instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify an instance, this command displays information about all instances.

id *instance-id*: Specifies an eMDI instance by its ID. If you do not specify an instance, this command displays information about all instances.

verbose: Displays detailed instance information. If you do not specify this keyword, the command displays brief instance information.

Examples

Display brief information about eMDI instance **eMDI1**.

```
<Sysname> display emdi instance name eMDI1
```

Status	Protocol	Type	Source IP/Port	Destination IP/Port
Active	TCP	Static	1.1.1.1/2001	2.2.2.2/2010

Display brief information about all eMDI instances.

```
<Sysname> display emdi instance
```

Brief information about all instances:

ID	Name	Type	Instance status	Protocol
1	eMDI1	Static	Active	TCP
2	-	Dynamic	Inactive	UDP

Display detailed information about eMDI instance **eMDI1**, which monitors a TCP data flow.

```
<Sysname> display emdi instance name eMDI1 verbose
```

Instance name : eMDI1

ID : 1

Instance status : Active

Protocol : TCP

Type : Static

Destination IP : 2.2.2.2

Destination port : 2010

Source IP : 1.1.1.1

Source port : 2001

VLAN ID : 45

VXLAN ID : -

VPN instance name : -

Monitoring period : 10 sec

Monitoring periods that passed : 30

Maximum sample packets per period : -

Lifetime : 10 hours

Running time : 8 hours 20 min 30 sec

Normal periods : 29

Abnormal periods : 1

UPLR : 1000

DPLR : 1000

Display detailed information about eMDI instance 2, which monitors a UDP data flow.

```
<Sysname> display emdi instance id 2 verbose
```

Instance name : -

ID : 2

Instance status : Inactive

Protocol : UDP

Type : Dynamic

Destination IP : 2.2.2.2

Destination port : 2010

Source IP : 1.1.1.1

Source port : 2001

VLAN ID : 45

VXLAN ID : -

```

VPN instance name           : -
Payload type                : -
Clock rate                  : 90000 Hz
Monitoring period           : 10 sec
Monitoring periods that passed : 30
Maximum sample packets per period : 100
Lifetime                    : 10 hours
Running time                : 8 hours 20 min 30 sec
Normal periods              : 29
Abnormal periods            : 1
RTP-LR                      : 100
RTP-SER                     : 100
FEC window                  : 100
FEC threshold               : 5

```

Table 85 Command output

Field	Description
Status Instance status	Instance status: • Active. • Inactive.
Protocol	Transport layer protocol of the data flow: • TCP. • UDP.
Type	Instance creation method: • Static—The eMDI instance was manually configured at the CLI. • Dynamic—The eMDI instance was created by other features.
Source IP/Port Source Port	Source IP address and source port of the data flow.
Destination IP/Port Destination Port	Destination IP address and destination port of the data flow.
ID	Instance ID.
Name/Instance name	Instance name.
VLAN ID	VLAN ID of the data flow.
VXLAN ID	VXLAN ID of the data flow.
VPN instance name	VPN instance name of the data flow.
Monitoring period	Instance monitoring period, in seconds.
Monitoring periods that passed	Number of passed monitoring periods. If the device did not receive packets of the data flow within some monitoring periods, the number of passed monitoring periods is greater than the total number of normal periods and abnormal periods .
Maximum sample packets per period	Maximum number of packets sampled per monitoring period in the instance.
Lifetime	Instance lifetime.
Running time	Instance running time. The value of this field might be slightly greater than the value of the

Field	Description
	lifetime field in the following situations: - The instance lifetime has expired but the current monitoring period has not. The instance will run until the current monitoring period expires. - The instance lifetime is long and the instance running time is reaching or has already reached the instance lifetime.
Normal periods	Number of periods when both the number of lost packets and the number of out-of-order packets were within the alarm thresholds.
Abnormal periods	Number of periods when the number of lost or out-of-order packets exceeded the alarm threshold.
UPLR	Alarm threshold for the upstream TCP packet loss rate.
DPLR	Alarm threshold for the downstream TCP packet loss rate.
Payload type	RTP packet payload type of the UDP data flow to be monitored.
Clock rate	RTP packet clock frequency of the UDP data flow to be monitored, in Hz.
RTP-LR	Alarm threshold for the RTP packet loss rate.
RTP-SER	Alarm threshold for the RTP sequence error rate.
FEC window	Sliding window size for UDP data flow quality monitoring.
FEC threshold	FEC packet loss threshold for UDP data flow quality monitoring.

display emdi resource

Use **display emdi resource** to display eMDI instance resource information.

Syntax

display emdi resource

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display eMDI instance resource information.

```
<Sysname> display emdi resource
```

```
Specifications(Slot 0):
```

```

Max instances                : 8
Max UDP instances            : 8
Max TCP instances            : 8
Max static instances         : 8
Max dynamic instances        : 8
```

```
Configuration(Slot 0):
```

```

Configured instances         : 0
Running instances            : 0
Running UDP instances        : 0
```

```

Running TCP instances           : 0
Running static instances       : 0
Running dynamic instances      : 0

```

Table 86 Command output

Field	Description
Specifications	Supported eMDI specifications.
Max instances	Maximum number of instances that can run at the same time.
Max UDP instances	Maximum number of UDP instances that can run at the same time.
Max TCP instances	Maximum number of TCP instances that can run at the same time.
Max static instances	Maximum number of static instances that can run at the same time.
Max dynamic instances	Maximum number of dynamic instances that can run at the same time.
Configuration	Current eMDI configuration.
Configured instances	Number of configured instances.
Running instances	Total number of running instances. Total number of running instances = Number of running UDP instances + Number of running TCP instances = Number of running static instances + Number of running dynamic instances .
Running UDP instances	Number of running instances that monitors UDP data flows.
Running TCP instances	Number of running instances that monitors TCP data flows.
Running static instances	Number of running static instances.
Running dynamic instances	Number of running dynamic instances.
Specifications and configuration	Supported eMDI specifications and current eMDI configuration.

Related commands

emdi

display emdi statistics

Use **display emdi statistics** to display monitoring statistics for an eMDI instance.

Syntax

```

display emdi statistics { instance-name instance-name | instance-id instance-id }
[ number number ] [ abnormal | verbose ]

```

Views

Any view

Predefined user roles

```

network-admin
network-operator

```

Parameters

instance-name *instance-name*: Specifies an eMDI instance by its name, a case-sensitive string of 1 to 31 characters.

instance-id *instance-id*: Specifies an eMDI instance by its ID.

number number: Displays statistics for the specified number of monitoring periods. The *number* argument is in the range of the 1 to 60. The default value is 3.

abnormal: Displays statistics for periods with lost or out-of-order packets. If you do not specify this keyword, the command displays statistics for both normal periods and abnormal periods.

verbose: Displays detailed monitoring statistics for the data flow. If you do not specify this keyword, the command displays brief monitoring statistics.

Usage guidelines

The device stores only the monitoring statistics within the most recent 60 monitoring periods for each eMDI instance.

If you specify both the **abnormal** keyword and the **number number** option, this command displays statistics for the specified number of abnormal periods.

Examples

Display brief monitoring statistics for eMDI instance **eMDI1**.

```
<Sysname> display emdi statistics instance-name eMDI1
Instance name      : eMDI1
Instance ID       : 1
Monitoring period: 10 sec
Protocol          : TCP
Unit for DPLR and UPLR is 1/100000
Timestamp          Status    Rate(bps)    DPLR    UPLR    DRTT(us)    URTT(us)
2019/09/17 16:17:20 Normal    4539000      0        0        2694        2315
2019/09/17 16:17:10 Abnormal  4865656    46786     0        3656        3711
2019/09/17 16:17:00 Abnormal  4865656    12362    4568     69564       26965
```

Display brief monitoring statistics for the most recent two monitoring periods of eMDI instance **eMDI2**.

```
<Sysname> display emdi statistics instance-name eMDI2 number 2
Instance name      : eMDI2
Instance ID       : 2
Monitoring period: 10 sec
Protocol          : UDP
Unit for RTP-LR, RTP-SER and RTP-ELF is 1/100000
Timestamp          Status    RTP-LR    RTP-SER    Jitter(us)    RTP-LP    RTP-ELF
2019/09/17 16:17:20 Normal     0         0         4294         0         0
2019/09/17 16:17:10 Abnormal  36533    25365     6729         15        12566
```

Display detailed monitoring statistics for eMDI instance **eMDI3**.

```
<Sysname> display emdi statistics instance-name eMDI3 verbose
Instance name      : eMDI3
Instance ID       : 3
Monitoring period  : 10 sec
Protocol          : UDP
Timestamp         : 2019-09-17 17:02:00
Service module    : Slot 1
Inbound interface : GigabitEthernet1/0/1
Flow status       : Abnormal
Received packets  : 3850
Rate             : 128 pps
Received bytes    : 5390000
```

Rate	: 1437333 bps
Lost packets	: 32261
RTP-LR	: 89338/100000
Packet out of sequence	: 0
RTP-SER	: 0/100000
RTP-LP	: 5
RTP-ELF	: 2/100000
Maximum jitter	: 8815 us
Average jitter	: 8540 us
Minimum jitter	: 8262 us
Timestamp	: 2019-09-17 17:01:50
Service module	: Slot 1
Inbound interface	: GigabitEthernet1/0/1
Flow status	: Normal
Received packets	: 3736
Rate	: 128 pps
Received bytes	: 5145000
Rate	: 1237333 bps
Lost packets	: 31481
RTP-LR	: 81569/100000
Packet out of sequence	: 0
RTP-SER	: 0/100000
RTP-LP	: 5
RTP-ELF	: 2/100000
Maximum jitter	: 7885 us
Average jitter	: 7564 us
Minimum jitter	: 7242 us
Timestamp	: 2019-09-17 17:01:40
Service module	: Slot 1
Inbound interface	: GigabitEthernet1/0/1
Flow status	: Normal
Received packets	: 3736
Rate	: 128 pps
Received bytes	: 5145000
Rate	: 1237333 bps
Lost packets	: 31481
RTP-LR	: 81569/100000
Packet out of sequence	: 0
RTP-SER	: 0/100000
RTP-LP	: 5
RTP-ELF	: 2/100000
Maximum jitter	: 7885 us
Average jitter	: 7564 us
Minimum jitter	: 7242 us

Display detailed monitoring statistics for the most recent monitoring period of eMDI instance **eMDI4**.

<Sysname> display emdi statistics instance-name eMDI4 number 1 verbose

Instance name : eMDI4
Instance ID : 4
Monitoring period : 10 sec
Protocol : TCP

Timestamp : 2019-09-17 17:02:00
Service module : Slot 1
Inbound interface : GigabitEthernet1/0/1
Flow status : Abnormal
Received packets : 95
Rate : 9 pps
Received bytes : 12510
Rate : 10008 bps
UPLC : 0
UPLR : 0/100000
DPLC : 0
DPLR : 0/100000
URTT : 35 us
DRTT : 8354549 us

Service module : Slot 2
Inbound interface : GigabitEthernet2/0/1
Flow status : Abnormal
Received packets : 95
Rate : 9 pps
Received bytes : 12510
Rate : 10008 bps
UPLC : 0
UPLR : 0/100000
DPLC : 0
DPLR : 0/100000
URTT : 35 us
DRTT : 8354549 us

Display statistics for abnormal periods of eMDI instance eMDI5.

<Sysname> display emdi statistics instance-name eMDI5 abnormal

Instance name : eMDI5
Instance ID : 5
Monitoring period : 10 sec
Protocol : TCP

Timestamp : 2019-09-17 17:02:00
Service module : Slot 1
Inbound interface : GigabitEthernet1/0/1
Flow status : Abnormal
Received packets : 95
Rate : 9 pps
Received bytes : 12510

```

Rate                : 10008 bps
UPLC                : 0
UPLR                : 0/100000
DPLC                : 0
DPLR                : 0/100000
URTT                : 35 us
DRTT                : 8354549 us

Timestamp           : 2019-09-17 17:00:00
Service module      : Slot 1
Inbound interface   : GigabitEthernet1/0/1
Flow status         : Abnormal
Received packets    : 95
Rate                : 9 pps
Received bytes      : 12510
Rate                : 10008 bps
UPLC                : 0
UPLR                : 0/100000
DPLC                : 0
DPLR                : 0/100000
URTT                : 35 us
DRTT                : 8354549 us

Timestamp           : 2019-09-17 16:58:00
Service module      : Slot 1
Inbound interface   : GigabitEthernet1/0/1
Flow status         : Abnormal
Received packets    : 95
Rate                : 9 pps
Received bytes      : 12510
Rate                : 10008 bps
UPLC                : 0
UPLR                : 0/100000
DPLC                : 0
DPLR                : 0/100000
URTT                : 35 us
DRTT                : 8354549 us

```

Table 87 Command output

Field	Description
Monitoring period	Monitoring period of the eMDI instance, in seconds.
Protocol	Transport layer protocol of the data flow: • TCP. • UDP.
Timestamp	Time when the statistics were recorded.
Status Flow status	Flow status: • Normal. • Abnormal.

Field	Description
Rate	Packet input rate, in bps or pps. If no packets of the data flow were received within the monitoring period, this field displays a hyphen (-).
DPLR	Downstream packet loss rate, in units of one hundred thousandth.
UPLR	Upstream packet loss rate, in units of one hundred thousandth.
DRTT	Average downstream round trip time, in microseconds.
URTT	Average upstream round trip time, in microseconds.
RTP-LR	RTP packet loss rate, in units of one hundred thousandth.
RTP-SER	RTP packet sequence error rate, in units of one hundred thousandth.
Jitter	RTP packet jitter, in microseconds.
RTP-LP	Maximum number of continuously lost RTP packets.
RTP-ELF	RTP effective loss factor for Forward Error Correct (FEC), in units of one hundred thousandth.
Service module	Number of the slot where the instance resides.
Inbound interface	Inbound interface of the packets.
Received packets	Number of received packets.
Received bytes	Bytes of received TCP or UDP packets.
Lost packets	Number of lost packets.
Packet out of sequence	Number of out-of-order packets.
Maximum jitter	Maximum jitter in microseconds.
Average jitter	Average jitter in microseconds.
Minimum jitter	Minimum jitter in microseconds.
UPLC	Upstream packet loss rate.
DPLC	Downstream packet loss rate.

emdi

Use **emdi** to enable eMDI and enter its view.

Use **undo emdi** to restore the default.

Syntax

emdi

undo emdi

Default

eMDI is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The **undo emdi** command disables eMDI and deletes all eMDI settings.

Examples

Enable eMDI and enter its view.

```
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi]
```

fec

Use **fec** to specify the sliding window size and packet loss threshold for a UDP data flow to be monitored.

Use **undo fec** to restore the default.

Syntax

fec { **window** *window-size* | **threshold** *threshold-value* } *

undo fec

Default

The sliding window size and packet loss threshold for a UDP data flow are 100 and 5, respectively.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

window *window-size*: Specifies the sliding window size in packets, in the range of 10 to 1000.

threshold *threshold-value*: Specifies the packet loss threshold in packets, in the range of 1 to 100.

Usage guidelines

This command enables you to monitor the packet loss conditions of the UDP data flow. After each window slide, the system identifies whether the number of lost data packets in the window within the monitoring period is greater than the threshold. If yes, the system increases RTP-ELF by 1. The window sliding stops when the monitoring period expires. If the total number of packet loss windows is greater than 0 within a monitoring period, a video fault exists.

This command is intended for a UDP data flow. Before executing this command, you must specify the UDP data flow for the eMDI instance to monitor.

The packet loss threshold must be smaller than the sliding window size.

To modify the FEC settings for an eMDI instance that is already started, you must stop the instance first by executing the **stop** command.

Examples

Set the sliding window size and packet loss threshold for eMDI instance **eMDI1** to 10 and 5, respectively.

```
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI1
[Sysname-emdi-instance-eMDI1] flow ipv4 udp source 10.0.0.1 destination 10.2.2.2
```

```
[Sysname-emdi-instance-EMDI1] fec window 10 threshold 5
```

Related commands

flow ipv4 udp

flow ipv4 tcp

Use **flow ipv4 tcp** to specify a TCP data flow to be monitored.

Use **undo flow** to restore the default.

Syntax

```
flow ipv4 tcp source source-ip-address destination destination-ip-address  
[ destination-port destination-port-number | source-port source-port-number | vlan vlan-id  
| vni vxlan-id | vpn-instance vpn-instance-name ] *
```

undo flow

Default

No TCP data flow is specified for an eMDI instance.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

source *source-ip address*: Specifies the source IP address of the data flow in dotted-decimal notation.

destination *destination-ip-address*: Specifies the destination IP address of the data flow in dotted-decimal notation.

destination-port *destination-port-number*: Specifies the destination port number of the data flow, in the range of 1 to 65535.

source-port *source-port-number*: Specifies the source port number of the data flow, in the range of 1 to 65535.

vlan *vlan-id*: Specifies the VLAN ID of the data flow, in the range of 1 to 4094.

vni *vxlan-id*: Specifies the VXLAN ID of the data flow, in the range of 0 to 16777215.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the data flow belongs to the public network.

Usage guidelines

You can specify a data flow by using any combination of the following items: source IP address, destination IP address, source port number, destination port number, VLAN ID, and VXLAN ID. Using more items defines a more granular data flow and provides more helpful monitoring data and analysis results.

For a VXLAN data flow, all parameters except VXLAN ID are used to match the fields in the inner packet header.

An eMDI instance can monitor only one data flow. A data flow can be monitored by only one eMDI instance.

If you execute this command multiple times when the eMDI instance is not started, the most recent configuration takes effect.

To modify the data flow configuration for an instance that is already started, you must stop the instance first by executing the **stop** command.

The **undo flow** command also restores the default eMDI alarm settings.

Examples

Configure eMDI instance **eMDI2** to monitor the TCP data flow from 10.0.0.1 to 10.0.0.2.

```
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI2
[Sysname-emdi-instance-eMDI2] flow ipv4 tcp source 10.0.0.1 destination 10.0.0.2
```

flow ipv4 udp

Use **flow ipv4 udp** to specify a UDP data flow to be monitored.

Use **undo flow** to restore the default.

Syntax

```
flow ipv4 udp source source-ip-address destination destination-ip-address
[ destination-port destination-port-number | source-port source-port-number | vlan vlan-id
| vni vxlان-id | pt pt-value | clock-rate clock-rate-value | vpn-instance vpn-instance-name ]
*
```

undo flow

Default

No UDP data flow is specified for an eMDI instance.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

source *source-ip address*: Specifies the source IP address of the data flow in dotted-decimal notation.

destination *destination-ip-address*: Specifies the destination IP address of the data flow in dotted-decimal notation.

destination-port *destination-port-number*: Specifies the destination port number of the data flow, in the range of 1 to 65535.

source-port *source-port-number*: Specifies the source port number of the data flow, in the range of 1 to 65535.

vlan *vlan-id*: Specifies the VLAN ID of the data flow, in the range of 1 to 4094.

vni *vxlان-id*: Specifies the VXLAN ID of the data flow, in the range of 0 to 16777215.

pt *pt-value*: Specifies the RTP packet payload type of the data flow, in the range of 25 to 71 or 77 to 127.

clock-rate *clock-rate-value*: Specifies the RTP packet clock frequency. The available values include 8000 Hz, 16000 Hz, and 90000 Hz. The default value is 90000 Hz. The specified RTP packet clock frequency must be the sampling frequency of the data flow. If not, the calculated jitter values cannot reflect the actual situation.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the data flow belongs to the public network.

Usage guidelines

You can specify a data flow by using any combination of the following items: source IP address, destination IP address, source port number, destination port number, VLAN ID, and VXLAN ID. Using more items defines a more granular data flow and provides more helpful monitoring data and analysis results.

For a VXLAN data flow, all parameters except VXLAN ID are used to match the fields in the inner packet header.

An eMDI instance can monitor only one data flow. A data flow can be monitored by only one eMDI instance.

If you execute this command multiple times when the eMDI instance is not started, the most recent configuration takes effect.

To modify the data flow configuration for an instance that is already started, you must stop the instance first by executing the **stop** command.

The **undo flow** command also restores the default eMDI alarm settings and FEC settings.

Examples

Configure eMDI instance **eMDI1** to monitor the UDP data flow from 10.0.0.1 to 10.0.0.2.

```
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI1
[Sysname-emdi-instance-eMDI1] flow ipv4 udp source 10.0.0.1 destination 10.0.0.2
```

instance

Use **instance** to create an eMDI instance and enter its view, or enter the view of an existing eMDI instance.

Use **undo instance** to delete an eMDI instance.

Syntax

instance *instance-name*

undo instance *instance-name*

Default

No eMDI instance exists.

Views

eMDI view

Predefined user roles

network-admin

Parameters

instance-name: Specifies the name for the eMDI instance, a case-sensitive string of 1 to 31 characters.

Usage guidelines

eMDI instances are fundamental elements of the eMDI feature. Each eMDI instance monitors one data flow as defined by its parameters, including the lifetime, monitoring period, and alarm thresholds.

A data flow can be monitored by only one eMDI instance.

To view the maximum number of eMDI instances that the device can run at the same time, execute the **display emdi resource** command.

Examples

```
# Create an eMDI instance named eMDI1.
```

```
<Sysname> system-view
```

```
[Sysname] emdi
```

```
[Sysname-emdi] instance eMDI1
```

Related commands

display emdi resource

lifetime

Use **lifetime** to specify the eMDI instance lifetime.

Use **undo lifetime** to restore the default.

Syntax

lifetime { **seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days* }

undo lifetime

Default

The eMDI instance lifetime is 1 hour.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

seconds *seconds*: Specifies the lifetime in seconds. The value range is 300 to 604800.

minutes *minutes*: Specifies the lifetime in minutes. The value range is 5 to 10080.

hours *hours*: Specifies the lifetime in hours. The value range is 1 to 168.

days *days*: Specifies the lifetime in days. The value range is 1 to 7.

Usage guidelines

An eMDI instance starts to operate after you use the **start** command to start it, and it stops when its lifetime expires.

To change the lifetime for an eMDI instance that is already started, you must stop the instance first by executing the **stop** command.

Examples

```
# Set the lifetime to 300 seconds for eMDI instance eMDI1.
```

```
<Sysname> system-view
```

```
[Sysname] emdi
```

```
[Sysname-emdi] instance eMDI1
```

```
[Sysname-emdi-instance-eMDI1] lifetime seconds 300
```

monitor-period

Use **monitor-period** to specify the monitoring period for an eMDI instance.

Use **undo monitor-period** to restore the default.

Syntax

monitor-period *period-value*

undo monitor-period

Default

The monitoring period for an eMDI instance is 60 seconds.

Views

eMDI instance view

Predefined user roles

network-admin

Parameters

period-value: Specifies the monitoring period, which can be 10, 30, or 60 seconds.

Usage guidelines

The eMDI instance obtains monitoring data from the device periodically.

To change the monitoring period for an eMDI instance that is already started, you must stop the instance first by executing the **stop** command.

Examples

Set the monitoring period to 10 seconds for eMDI instance **eMDI1**.

```
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI1
[Sysname-emdi-instance-eMDI1] monitor-period 10
```

monitor-period-packet maximum

Use **monitor-period-packet maximum** to configure the maximum number of packets sampled per monitoring period for eMDI instances.

Use **undo monitor-period-packet maximum** to restore the default.

Syntax

monitor-period-packet maximum *max-number*

undo monitor-period-packet maximum

Default

All matching packets are sampled per monitoring period for eMDI instances.

Views

eMDI view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of packets sampled per monitoring period in the range of 64 to 65535.

Usage guidelines

For an eMDI instance, if the number of matching packets within a monitoring period exceeds the maximum number specified by using this command, the excess packets will not be monitored.

The number of matching packets for an eMDI instance per monitoring period depends on the following factors:

- The number of packets collected by the device.
- The match criteria of the destination data flow configured by using the **flow ipv4 tcp** or **flow ipv4 udp** command.
- The monitoring period of the eMDI instance configured by using the **monitor-period** command.

This command takes effect on all eMDI instances of the device.

Examples

Set the maximum number of packets sampled per monitoring period to 100 for all eMDI instances.

```
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] monitor-period-packet maximum 100
```

reset emdi statistics

Use **reset emdi statistics** to clear eMDI statistics.

Syntax

reset emdi statistics [**instance-name** *instance-name* | **instance-id** *instance-id-value*]

Views

User view

Predefined user roles

network-admin

Parameters

instance *instance-name*: Specifies an instance by its name, a case-sensitive string of 1 to 31 characters.

instance-id *instance-id*: Specifies an instance by its ID. If you do not specify this option, this command displays information about all instances.

Usage guidelines

If you do not specify the **instance** *instance-name* or **instance-id** *instance-id* option, this command clears statistics about all static instances.

The dynamic instance is identified only by its ID. With the **instance** *instance-name* option specified, this command clears statistics about the specified static instance.

With the **instance-id** *instance-id* option specified, this command clears statistics about the specified instances whatever the instance is static or dynamic.

Examples

Clear statistics about eMDI instance **eMDI1**.

```
<Sysname> reset emdi statistics instance-name eMDI1
```


Related commands

display emdi statistics

start

Use **start** to start an eMDI instance.

Syntax

start

Views

eMDI instance view

Predefined user roles

network-admin

Usage guidelines

A started eMDI instance automatically stops upon a master/subordinate or active/standby switchover. You must execute this command again to start the instance.

To modify the configuration for an eMDI instance that is already started, stop the instance first by executing the **stop** command.

Examples

```
# Start eMDI instance eMDI2.
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI2
[Sysname-emdi-instance-eMDI2] flow ipv4 udp source 10.0.0.1 destination 10.0.0.2
[Sysname-emdi-instance-eMDI2] start
```

Related commands

flow ipv4 tcp

flow ipv4 udp

stop

Use **stop** to stop an eMDI instance.

Syntax

stop

Views

eMDI instance view

Predefined user roles

network-admin

Examples

```
# Stop eMDI instance eMDI2.
<Sysname> system-view
[Sysname] emdi
[Sysname-emdi] instance eMDI2
```

```
[Sysname-emdi-instance-EMDI2] stop
```

stop all

Use **stop all** to stop all eMDI instances.

Syntax

stop all

Views

eMDI view

Predefined user roles

network-admin

Usage guidelines

This command stops all running static instances.

Examples

```
# Stop all eMDI instances.  
<Sysname> system-view  
[Sysname] emdi  
[Sysname-emdi] stop all
```

New feature: Enabling SNMP notifications for OpenFlow

Enabling SNMP notifications for OpenFlow

About this task

This feature enables OpenFlow to generate SNMP notifications for important OpenFlow events. For the notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.
system-view
2. Enable SNMP notifications for OpenFlow.
snmp-agent trap enable openflow [connect-state]
By default, SNMP notifications are enabled for OpenFlow.

Command reference

New command: snmp-agent trap enable openflow

Use **snmp-agent trap enable openflow** to enable SNMP notifications for OpenFlow.

Use **undo snmp-agent trap enable openflow** to disable SNMP notifications for OpenFlow.

Syntax

```
snmp-agent trap enable openflow [ connect-state ]  
undo snmp-agent trap enable openflow [ connect-state ]
```

Default

SNMP notifications are enabled for OpenFlow.

Views

System view

Predefined user roles

network-admin

Parameters

connect-state: Specifies notifications about status changes of the connections between OpenFlow switches and controllers. If you do not specify this keyword, the command enables all notifications for OpenFlow.

Usage guidelines

This command enables OpenFlow to generate SNMP notifications for important OpenFlow events. For the notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

```
# Enable SNMP notifications for OpenFlow.  
<Sysname> system-view  
[Sysname] snmp-agent trap enable openflow
```

New feature: EVPN VPLS

About EVPN VPLS

EVPN Virtual Private LAN Service (VPLS) is a Layer 2 VPN technology that uses MP-BGP to advertise EVPN routes in the control plane and MPLS for forwarding in the data plane. EVPN VPLS provides point-to-multipoint forwarding services for users with MAC address table lookup in VSIs.

EVPN VPLS network model

As shown in [Figure 46](#), an EVPN VPLS network contains the following devices:

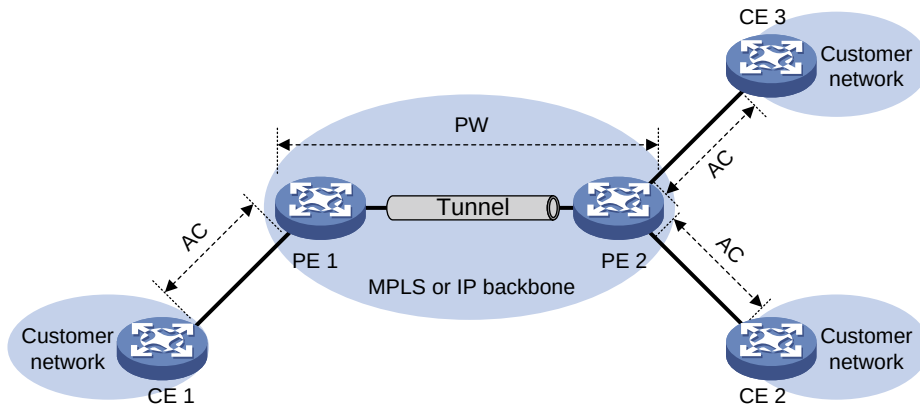
- **Customer edge (CE)**—Customer device directly connected to the service provider network.
- **Provider edge (PE)**—Service provider device connected to CEs. PEs provide access to the EVPN VPLS network and forward traffic between customer network sites by using public tunnels.

A PE uses ACs, PWs, tunnels, and VSIs to provide EVPN VPLS services.

- **Attachment circuit (AC)**—A physical or virtual link between a CE and a PE.
- **Pseudowire (PW)**—A pair of unidirectional virtual connections in opposite directions between two PEs.
- **Public tunnel**—A connection that carries one or more PWs across the MPLS or IP backbone. A public tunnel can be an LSP, GRE, or MPLS TE tunnel.
- **Virtual Switch Instance (VSI)**—A virtual switch instance provides Layer 2 switching services for a VPLS instance (EVPN instance) on a PE. A VSI acts as a virtual switch that has all the functions of a

conventional Ethernet switch, including source MAC address learning, MAC address aging, and flooding. VPLS uses VSIs to forward Layer 2 data packets in EVPN instances.

Figure 46 EVPN VPLS network



Neighbor auto-discovery and PW establishment

A PE uses IMET routes to automatically discover neighbors and establish PWs. When a PE receives an IMET route in a VSI, it compares the export route targets of the route with the import route targets of the EVPN instance associated with the VSI. If they match, the PE will establish a unidirectional virtual connection based on the PE address and PW label information carried in the route. PW establishment is finished when two virtual connections in opposite directions are established between two PEs.

MAC address learning, aging, and withdrawal

Source MAC address learning

A PE uses the MAC address table of a VSI to forward Layer 2 unicast traffic for that VSI.

A PE learns source MAC addresses in the following ways:

- **Local MAC address learning**—When the PE receives a frame from a local CE, it first identifies the VSI of the frame. Then, the PE adds the source MAC address of the frame (the MAC address of the local CE) to the MAC address table of the VSI. The output interface of the MAC address entry is the AC that receives the frame.
- **Remote MAC address learning**—A PE advertises the MAC addresses of local CEs to remote PEs through BGP EVPN MAC/IP advertisement routes. When a remote PE receives the routes, it adds the received MAC addresses to the MAC address table of the corresponding VSI. The output interface is the PW.

MAC address aging

- **Local MAC address aging**—The MAC address table uses an aging timer for each dynamic MAC address entry. If no packet is received from a MAC address before the aging timer expires, VPLS deletes the MAC address.
- **Remote MAC address aging**—Remote MAC addresses advertised through MAC/IP advertisement routes are not removed from the MAC address table until routes to withdraw the MAC addresses are received.

MAC address withdrawal

When an AC goes down, the PE deletes MAC addresses on the AC. Then it sends an LDP address withdrawal message to notify all other PEs in the EVPN instance to delete those MAC addresses.

Traffic forwarding and flooding

Unicast traffic forwarding

After a PE receives a unicast packet with a known destination MAC address from an AC, the PE searches the MAC address table of the VSI bound to the AC for packet forwarding.

- If the output interface in the entry is a PW, the PE inserts the PW label of the PW to the packet, and adds the public tunnel header to the packet. It then forwards the packet to the remote PE over the PW. If the public tunnel is an LSP or MPLS TE tunnel, each packet on the PW contains two labels. The inner label is the PW label, which identifies the PW and ensures that the packet is forwarded to the correct VSI. The outer label is the public LSP or MPLS TE tunnel label, which ensures that the packet is correctly forwarded to the remote PE.
- If the output interface in the entry is a local interface, the PE directly forwards the packet to the local interface.

After a PE receives a unicast packet with a known destination MAC address from a PW, the PE searches the MAC address table of the VSI bound to the PW for packet forwarding. The PE forwards the packet through the output interface in the matching MAC address entry.

Flooding

When a PE receives flood traffic from an AC in a VSI, it will flood the traffic to the following interfaces:

- All ACs in the VSI except for the incoming AC.
- All PWs associated with the VSI.

When a PE receives flood traffic from a PW, it will flood the traffic to all ACs in the VSI bound to the PW.

Full mesh and split horizon

A Layer 2 network requires a loop prevention protocol such as STP to avoid loops. However, a loop prevention protocol on PEs brings management and maintenance difficulties. Therefore, EVPN VPLS uses the following methods to prevent loops:

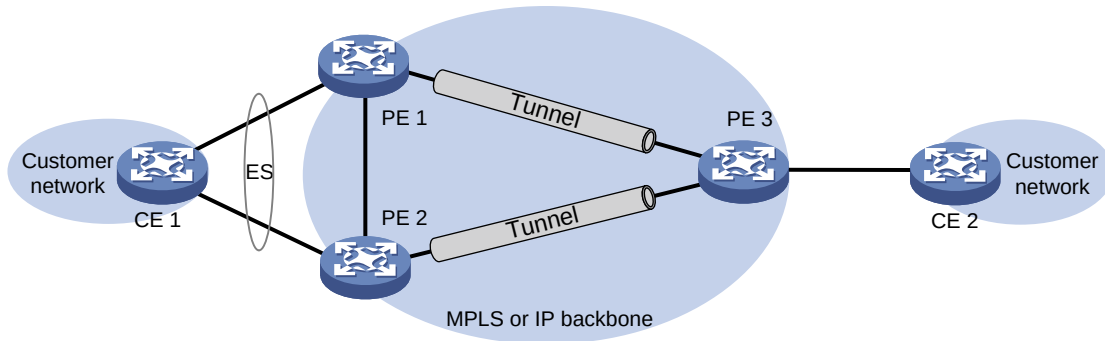
- **Full mesh**—Every two PEs in an EVPN instance must establish PWs. The PWs form a full mesh among PEs in the EVPN instance.
- **Split horizon**—A PE does not forward packets received from a PW to any other PWs in the same VSI but only forwards those packets to ACs.

EVPN VPLS multihoming

About EVPN VPLS multihoming

As shown in [Figure 47](#), EVPN VPLS supports deploying multiple PEs at a site for redundancy and high availability. On the redundant PEs, Ethernet links connected to the site form an ES that is uniquely identified by an ESI. EVPN VPLS supports only dualhoming.

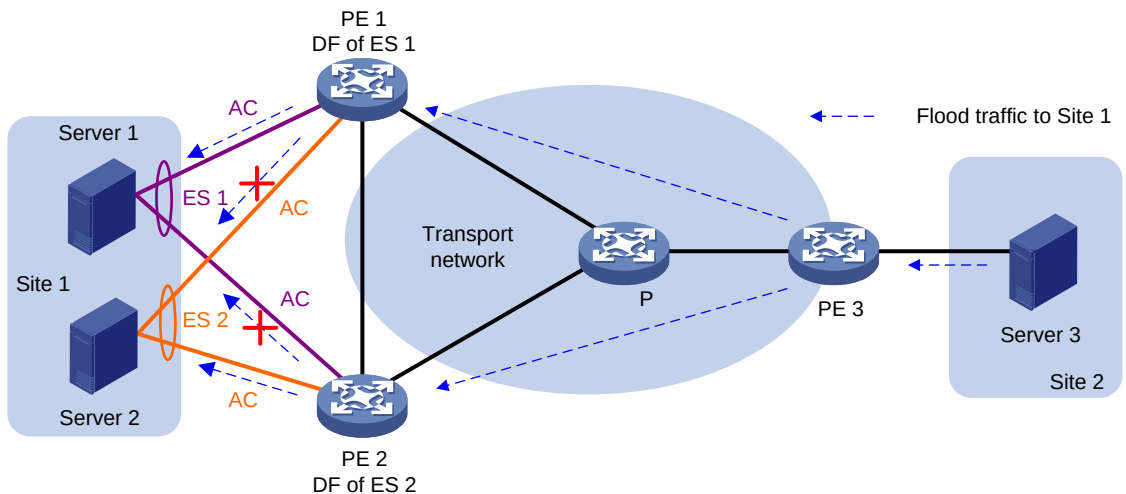
Figure 47 EVPN VPLS multihoming



DF election

To prevent redundant PEs from sending duplicate flood traffic to a multihomed site, a designated forwarder (DF) is elected from the PEs to forward flood traffic to the local site. PEs that fail the election are assigned the backup designated forwarder (BDF) role. BDFs do not forward flood traffic to the local site.

Figure 48 DF election



DF election can be performed by using a VLAN tag-based algorithm or preference-based algorithm.

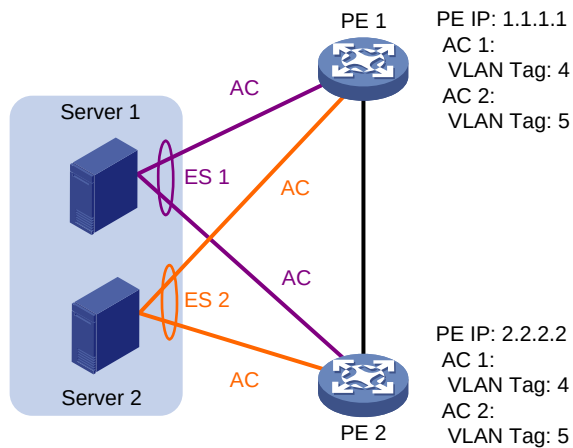
- VLAN tag-based DF election**

PEs select a DF for each AC based on the VLAN tag and PE IP address as follows:

- Arrange source IP addresses in Ethernet segment routes with the same ESI in ascending order and assign a sequence number to each IP address, starting from 0.
 - Divide the lowest VLAN ID permitted on an AC by the number of the redundant PEs, and match the remainder to the sequence numbers of IP addresses.
 - Assign the DF role to the PE that uses the IP address with the matching sequence number.
- The following uses PE 1 and PE 2 in Figure 49 as an example to explain the DF election procedure:
- PE 1 and PE 2 send Ethernet segment routes to each other.
 - The PEs assign sequence numbers 0 and 1 to IP addresses 1.1.1.1 and 2.2.2.2 in the Ethernet segment routes, respectively.
 - The PEs divide 4 (the lowest VLAN ID permitted by the ACs) by 2 (the number of redundant PEs), and match the remainder 0 to the sequence numbers of the IP addresses.

g. The DF role is assigned to PE 1 at 1.1.1.1.

Figure 49 VLAN tag-based DF election



- Preference-based DF election

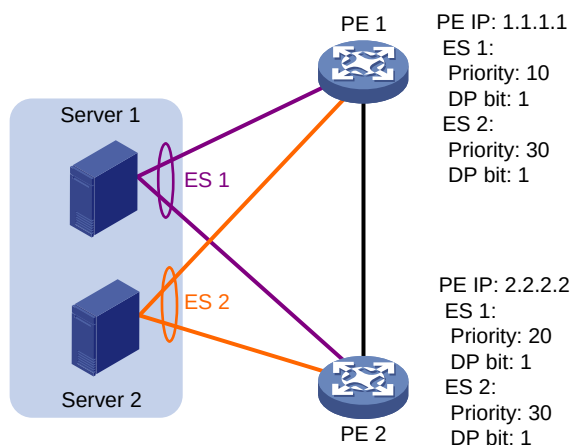
PEs select a DF for each ES based on the DF election preference, the Don't Preempt Me (DP) bit in Ethernet segment routes, and PE IP address. The DP bit can be set to one of the following values:

- **1**—Non-revertive mode is enabled for preference-based DF election (DF preemption is disabled). A DF retains its role when a new DF is elected.
- **0**—Non-revertive mode is disabled for preference-based DF election (DF preemption is enabled).

Preference-based DF election uses the following rules to select a DF for an ES:

- h. The PE with higher preference becomes the DF.
 - i. If two PEs have the same preference, the PE with the DP bit set to 1 becomes the DF.
 - j. If both of the PEs have the DP bit set to 1, the PE with a lower IP address becomes the DF.
- As shown in [Figure 50](#), PE 2 is the DF for ES 1, and PE 1 is the DF for ES 2.

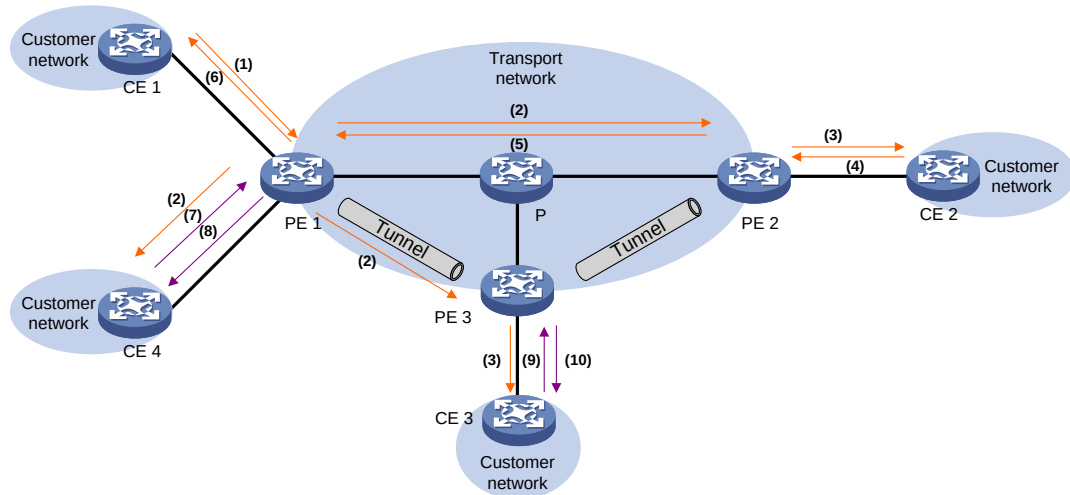
Figure 50 Preference-based DF election



Redundancy mode

The device supports single-active redundancy mode and all-active redundancy mode of EVPN VPLS multihoming.

Figure 52 ARP flood suppression



ARP flood suppression uses the following workflow:

2. CE1 sends an ARP request to obtain the MAC address of CE 2.
3. PE 1 creates a suppression entry for CE 1, floods the ARP request to local CEs and remote PEs (PE 2 and PE 3) in the VSI, and sends the suppression entry to PE 2 and PE 3 through BGP EVPN. Unicast-mode flooding is used to illustrate the workflow.
4. PE 2 and PE 3 de-encapsulate the ARP request and broadcast the request to local CEs in the VSI.
5. CE 2 sends an ARP reply after it receives the ARP request.
6. PE 2 creates a suppression entry for CE 2, forwards the ARP reply to PE 1, and sends the suppression entry to PE 1 and PE 3 through BGP EVPN.
7. PE 1 de-encapsulates the ARP reply and forwards the ARP reply to CE 1.
8. CE 4 sends an ARP request to obtain the MAC address of CE 1.
9. PE 1 creates a suppression entry for CE 4 and replies to the ARP request.
10. CE 3 sends an ARP request to obtain the MAC address of CE 1.
11. PE 3 creates a suppression entry for CE 3 and replies to the ARP request.

Control word

The control word field is between the MPLS label stack and the Layer 2 data. It carries control information for the Layer 2 frame, for example, the sequence number.

The control word feature has the following functions:

- Avoids fragment disorder. In multipath forwarding, fragments received might be disordered. The control word feature reorders the fragments according to the sequence number carried in the control word field.
- Identifies the original payload length for packets that include padding.

The control word field is optional for EVPN VPLS. You can configure whether to carry the control word field in packets sent on PWs. If you enable the control word feature on PEs at both ends of a PW, packets transmitted on the PW carry the control word field. Otherwise, the packets do not carry the control word field.

MAC mobility

MAC mobility refers to the movement of a VM or host from one ES to another. The source PE is unaware of the MAC move event. To notify other PEs of the change, the destination PE advertises a MAC/IP advertisement route for the MAC address. The source PE withdraws the old route for the MAC address after receiving the new route. The MAC/IP advertisement route has a sequence number that increases when the MAC address moves. The sequence number identifies the most recent move if the MAC address moves multiple times.

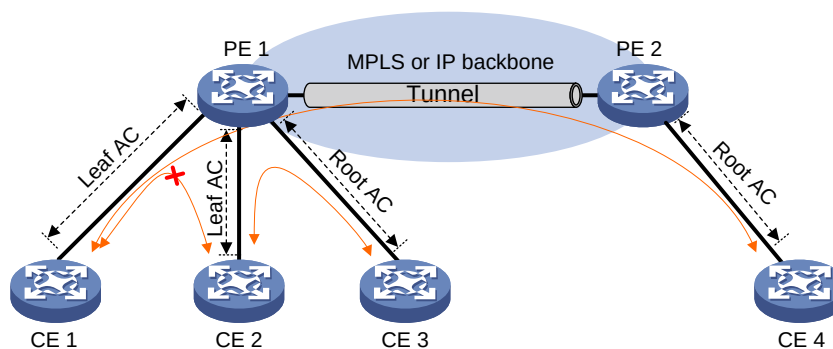
EVPN E-tree

About EVPN E-tree

In an EVPN VPLS network, EVPN E-tree isolates unicast and flood traffic (broadcast, multicast, and unknown unicast) of ACs in the same EVPN instance based on the AC roles. With EVPN E-tree, the device isolates unicast and flood traffic of ACs in the same EVPN instance as follows:

- Leaf ACs can access root ACs.
- Leaf ACs cannot access each other.
- Root ACs can access each other and access leaf ACs.

Figure 53 EVPN E-tree network diagram



Local traffic isolation

EVPN E-tree isolates traffic between local ACs on a PE as follows:

- When the PE receives packets from a leaf AC on a VSI, it forwards the packets only to root ACs on the VSI.
- When the PE receives packets from a root AC on a VSI, it forwards the packets to all local ACs on the VSI except the incoming AC.

Remote known unicast traffic isolation

With EVPN E-tree, PEs perform MAC address learning for hosts attached to leaf ACs as follows:

1. When a PE receives a packet from a leaf AC, it learns the source MAC address of the packet and adds the Leaf flag to the MAC address.
2. The PE advertises the MAC address to the remote PE in a MAC/IP advertisement route. The route carries the E-tree extended community attribute that contains the Leaf flag.
3. The remote PE adds the MAC address that carries the Leaf flag to the MAC address table.

When one PE receives a packet destined for a host on another PE from a local AC, it searches the MAC address table for the destination MAC address. If the entry of the destination MAC address has the Leaf flag and the packet is also from a leaf AC, the PE discards the packet. In other situations, the PE forwards the packet.

Remote flood traffic isolation

With EVPN E-tree, a PE assigns a Leaf label to the leaf ACs of each VSI. The PE adds the Leaf label to the E-tree extended community attribute in Ethernet auto-discovery routes and advertises the routes to remote PEs.

EVPN E-tree isolates flood traffic from one PE to another PE as follows:

1. When a PE receives a flood packet from a leaf AC on a VSI, it adds the Leaf label of that VSI to the packet, and then adds the private network label and public network label to the packet. After that, the PE forwards the packet to the remote PE.
2. The remote PE removes the private network label and public network label and finds the Leaf label. Then, the PE forwards the packet only to local root ACs on the same VSI.

EVPN VPLS tasks at a glance

To configure EVPN VPLS, perform the following tasks:

1. Configuring a VSI
 - a. Creating a VSI
 - b. (Optional.) Configure VSI parameters
2. Configuring an EVPN instance
3. Mapping a Layer 3 interface to a VSI
4. Configuring BGP to advertise BGP EVPN routes
 - a. Enabling BGP to advertise BGP EVPN routes
 - b. Enabling advertisement of MPLS-encapsulated BGP EVPN routes
 - c. (Optional.) Configuring optimal route selection and route advertisement settings
 - d. (Optional.) Maintaining BGP sessions
1. (Optional.) **错误!未找到引用源。**
5. (Optional.) Configuring EVPN VPLS multihoming
 - a. Assigning an ESI to an interface
 - b. (Optional.) Configuring the DF election algorithm
 - c. (Optional.) Setting the DF election delay
 - d. (Optional.) Setting the advertisement delay timer for Ethernet auto-discovery routes
 - e. (Optional.) Configuring local FRR for EVPN VPLS
 - f. (Optional.) Generating MAC address entries for received MAC/IP advertisement routes
 - g. (Optional.) Enabling VSIs to ignore the state of ACs
 - h. (Optional.) Disabling advertisement of EVPN multihoming routes
 - i. (Optional.) Ignoring the Ethernet tag on advertisement of Ethernet auto-discovery and MAC/IP advertisement routes
 - j. (Optional.) Enabling the device to monitor the BGP peer status of another local edge device
6. (Optional.) Managing remote MAC address entries and remote ARP learning
 - o Disabling MAC address advertisement
 - o Disabling learning of MAC addresses from ARP information
 - o Disabling ARP information advertisement
7. (Optional.) Enabling EVPN E-tree
8. (Optional.) Optimizing and maintaining an EVPN VPLS network:
 - o Confining floods to the local site

- Enabling ARP flood suppression
- Enabling packet statistics for an AC
- Enabling SNMP notifications for L2VPN PWs

Restrictions and guidelines: EVPN VPLS configuration

The device does not support S-trunk.

EVPN VPLS is mutually exclusive with EVPN-DCI dualhoming. Do not use the **evpn edge group** command in an EVPN VPLS network. For more information about EVPN-DCI dualhoming and the **evpn edge group** command, see "Configuring EVPN-DCI."

Configuring a VSI

Creating a VSI

1. Enter system view.
system-view
2. Enable L2VPN.
l2vpn enable
By default, L2VPN is disabled.
3. Create a VSI and enter VSI view.
vsi *vsi-name*
4. Bring up the VSI.
undo shutdown
By default, a VSI is not administratively down.

Configure VSI parameters

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Configure a VSI description.
description *text*
By default, a VSI does not have a description.
4. Set the MTU of the VSI.
mtu *mtu*
The default MTU for a VSI is 1500 bytes.
5. Set the maximum bandwidth for known unicast traffic of the VSI.
bandwidth *bandwidth*
By default, the maximum bandwidth is not limited for known unicast traffic of a VSI.
6. Set the broadcast, multicast, or unknown unicast bandwidth restraints of the VSI.
restrain { **broadcast** | **multicast** | **unknown-unicast** } *bandwidth*
The default for this command varies by device model.

7. Configure MAC address learning features for the VSI:
 - a. Enable MAC address learning for the VSI.
mac-learning enable
By default, MAC address learning is enabled for a VSI.
 - b. (Optional.) Set a limit for the VSI's MAC address table.
mac-table limit *mac-limit*
By default, no limit is set for a VSI's MAC address table.
 - c. (Optional.) Enable the VSI to drop source-unknown unicast frames if the MAC address table is full.
mac-table limit drop-unknown
By default, the VSI forwards source-unknown unicast frames without learning the source MAC address if the MAC address table is full.

Configuring an EVPN instance

About this task

The BGP EVPN routes advertised by a PE carry the RD and route targets configured for the EVPN instance of the routes.

You can configure routing policies in VSI EVPN instance view. An import routing policy is used for filtering the BGP EVPN routes received by the EVPN instance, and an export routing policy is used for filtering the BGP EVPN routes advertised by the EVPN instance.

Restrictions and guidelines

You can bind a VSI only to one EVPN instance.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Create an EVPN instance and enter VSI EVPN instance view.
evpn encapsulation mpls
4. Configure an RD for the EVPN instance.
route-distinguisher *route-distinguisher*
By default, no RD is configured for an EVPN instance.
5. Configure route targets for the EVPN instance.
vpn-target { *vpn-target*<1–8> | **auto** } [**both** | **export-extcommunity** | **import-extcommunity**]
By default, an EVPN instance does not have route targets.

Parameter	Description
export-extcommunity	Do not specify the same export targets for the EVPN instances of different VSIs. Do not specify the same export targets for the EVPN instances created in different views (system view, VSI view, VPN instance view, public instance view, and cross-connect group view).

Parameter	Description
	As a best practice, the export targets configured for the following objects do not match the import targets configured for the EVPN instances created in cross-connect group view: •VPN instances. •The public instance. •EVPN instances created in VSI view, VPN instance view, and public instance view.
import-extcommunity	As a best practice, the import targets configured for the following objects do not match the export targets configured for the EVPN instances created in cross-connect group view: •VPN instances. •The public instance. •EVPN instances created in VSI view, VPN instance view, and public instance view.

- (Optional.) Apply a PW class to the EVPN instance.
pw-class *class-name*
By default, no PW class is applied to an EVPN instance.
The specified PW class applies to all PWs in the EVPN instance.
- (Optional.) Apply a tunnel policy to the EVPN instance.
tunnel-policy *tunnel-policy-name*
By default, no tunnel policy is applied to an EVPN instance.
- (Optional.) Apply an export routing policy to the EVPN instance.
export route-policy *route-policy*
By default, no export routing policy is applied to an EVPN instance. The EVPN instance does not filter advertised routes.
- (Optional.) Apply an import routing policy to the EVPN instance.
import route-policy *route-policy*
By default, no import routing policy is applied to an EVPN instance. The EVPN instance accepts a route when the export route targets of the route match local import route targets.

Mapping a Layer 3 interface to a VSI

About this task

To assign the customer traffic on a Layer 3 interface to a VSI, map that interface to the VSI. The VSI uses its MAC address table to forward the customer traffic.

For more information about the commands in this task, see VPLS in *MPLS Command Reference*.

Procedure

- Enter system view.
system-view
- Enter Layer 3 interface view.
interface *interface-type interface-number*
- Map the Layer 3 interface to a VSI.
xconnect vsi *vsi-name* [**access-mode** { **ethernet** | **vlan** }] [**track** *track-entry-number*&<1-3>]
By default, a Layer 3 interface is not mapped to a VSI.

Configuring BGP to advertise BGP EVPN routes

Restrictions and guidelines for BGP EVPN route advertisement

For more information about BGP commands in this task, see *Layer 3—IP Routing Command Reference*.

Enabling BGP to advertise BGP EVPN routes

1. Enter system view.
system-view
2. Configure a global router ID.
router id router-id
By default, no global router ID is configured.
3. Enable a BGP instance and enter BGP instance view.
bgp as-number [instance instance-name]
By default, BGP is disabled and no BGP instances exist.
4. Specify remote PEs as BGP peers.
peer { group-name | ipv4-address [mask-length] } as-number as-number
5. Create the BGP EVPN address family and enter BGP EVPN address family view.
address-family l2vpn evpn
6. Enable BGP to exchange BGP EVPN routes with a peer or peer group.
peer { group-name | ipv4-address [mask-length] } enable
By default, BGP does not exchange BGP EVPN routes with peers.

Enabling advertisement of MPLS-encapsulated BGP EVPN routes

About this task

Perform this task on PEs for them to establish PWs.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP EVPN address family view.
address-family l2vpn evpn
4. Enable MPLS encapsulation for the BGP EVPN routes advertised to a peer or peer group.
peer { group name | ipv4-address [mask-length] | ipv6-address [prefix-length] } advertise encap-type mpls
By default, BGP EVPN routes use VXLAN encapsulation.

Configuring optimal route selection and route advertisement settings

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP EVPN address family view.
address-family **l2vpn evpn**
4. Permit the local AS number to appear in routes from a peer or peer group and set the number of appearances.
peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop** [*number*]
By default, the local AS number is not allowed in routes from peers.
5. Enable route target filtering for BGP EVPN routes.
policy vpn-target
By default, route target filtering is enabled for BGP EVPN routes.
6. Set a high priority for BGP routes learned from a peer or peer group during optimal route selection.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } **high-priority**
By default, BGP does not prefer routes learned from any peer or peer groups during optimal route selection.
7. Configure BGP route reflection settings:
 - a. Configure the device as an RR and specify a peer or peer group as its client.
peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**
By default, no RR or client is configured.
 - b. (Optional.) Enable BGP EVPN route reflection between clients.
reflect between-clients
By default, BGP EVPN route reflection between clients is enabled.
 - c. (Optional.) Configure the cluster ID of the RR.
reflector cluster-id { *cluster-id* | *ipv4-address* }
By default, an RR uses its own router ID as the cluster ID.
 - d. (Optional.) Create a reflection policy for the RR to filter reflected BGP EVPN routes.
rr-filter { *ext-comm-list-number* | *ext-comm-list-name* }
By default, an RR does not filter reflected BGP EVPN routes.
 - e. (Optional.) Create a reflection policy for the RR to filter reflected BGP EVPN routes.
reflect change-path-attribute
By default, an RR does not filter reflected BGP EVPN routes.
8. Configure the device to not change the next hop of routes advertised to an EBGp peer or peer group.
peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-invariable**
By default, the device uses its address as the next hop of routes advertised to EBGp peers.
9. Apply a routing policy to routes received from or advertised to a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** *route-policy-name*
{ **export** | **import** }

By default, no routing policies are applied to routes received from or advertised to peers or peer groups.

10. Advertise the COMMUNITY attribute to a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**

By default, the COMMUNITY attribute is not advertised to a peer or peer group.

11. Configure the BGP additional path feature.

- Configure the BGP additional path capabilities.

peer { *group-name* | *ipv4-address* [*mask-length*] } **additional-paths** { **receive** | **send** } *

By default, no BGP additional path capabilities are configured.

- Set the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise additional-paths best number**

By default, a maximum number of one Add-Path optimal route can be advertised to a peer or peer group.

- Set the maximum number of Add-Path optimal routes that can be advertised to all peers.

additional-paths select-best best-number

By default, a maximum number of one Add-Path optimal route can be advertised to all peers.

Maintaining BGP sessions

Perform the following tasks in user view:

- Reset BGP sessions of the BGP EVPN address family.

reset bgp [**instance** *instance-name*] { *as-number* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } | **all** | **external** | **group** *group-name* | **internal** } **l2vpn evpn**

- Soft-reset BGP sessions of the BGP EVPN address family.

refresh bgp [**instance** *instance-name*] { *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] } | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** } **l2vpn evpn**

Configuring a PW class

About this task

In a PW class, you can configure PW attributes such as the PW data encapsulation type, and whether to enable control word. To simplify PW attribute configuration for PWs, you can configure a PW class and apply the PW class to the PWs.

Restrictions and guidelines

Make sure the same data encapsulation type is configured for the two PEs that are connected by the same PW.

For correct PW setup, make sure the status of the control word feature is the same on the two PEs that are connected by the same PW.

For more information about PW class commands, see MPLS L2VPN in *MPLS Command Reference*.

Procedure

1. Enter system view.
system-view
2. Create a PW class and enter PW class view.
pw-class *class-name*
3. Enable control word.
control-word enable
By default, control word is disabled.
4. Specify the PW data encapsulation type.
pw-type { **ethernet** | **vlan** }
By default, the PW data encapsulation type is VLAN.
Support for parameters in this command depends on device model.

Configuring EVPN VPLS multihoming

Restrictions and guidelines for EVPN VPLS multihoming

In a multihomed site, AC configuration must be consistent on redundant PEs of the same ES.

You can assign an ESI to a main interface or a subinterface.

- For a subinterface, the ESI assigned to the subinterface takes precedence over that assigned to its main interface. If an ESI is assigned to a subinterface, the ES-related settings configured on the subinterface take effect, including the **evpn df-election algorithm**, **evpn df-election preference**, **evpn df-election preference non-revertive**, and **evpn timer es-delay** commands.
- If you assign an ESI only to a main interface, its subinterfaces inherit the ESI and ES settings of the main interface. The ES-related settings configured on the subinterface cannot take effect.

Assigning an ESI to an interface

About this task

An ESI uniquely identifies an ES. The links on interfaces with the same ESI belong to the same ES. Traffic of the ES can be distributed among the links for load sharing.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
 - Enter Layer 2 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*
 - Enter Layer 3 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.

interface route-aggregation *interface-number*

3. Assign an ESI to the interface.

esi *esi-id*

By default, no ESI is assigned to an interface.

Configuring the DF election algorithm

About this task

At a multihomed EVPN network site, you can modify the DF election algorithm to control the DF election result.

Restrictions and guidelines

You can configure the DF election algorithm in system view and in interface view. The global DF election algorithm takes effect on all ESS, and the interface-specific DF election algorithm takes effect only on the ESS on an interface. The interface-specific DF election algorithm takes precedence over the global DF election algorithm.

Configuring the DF election algorithm globally

1. Enter system view.

system-view

2. Configure the DF election algorithm.

evpn df-election algorithm *algorithm*

By default, the VLAN tag-based algorithm is used for DF election.

Configuring the DF election algorithm on an interface

1. Enter system view.

system-view

2. Enter interface view.

- Enter Layer 2 Ethernet interface view.

interface *interface-type interface-number*

- Enter Layer 2 aggregate interface view.

interface bridge-aggregation *interface-number*

- Enter Layer 3 Ethernet interface view.

interface *interface-type interface-number*

- Enter Layer 3 aggregate interface view.

interface route-aggregation *interface-number*

3. Configure the DF election algorithm.

evpn df-election algorithm *algorithm*

By default, the DF election algorithm specified in system view takes effect.

Configuring parameters for preference-based DF election

1. Enter system view.

system-view

2. Enter interface view.
 - Enter Layer 2 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*
 - Enter Layer 3 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.
interface route-aggregation *interface-number*
3. Set the DF election preference.
evpn df-election preference *preference*
By default, the DF election preference is 32767.
The larger the value, the higher the preference.
4. (Optional.) Enable non-revertive mode for preference-based DF election.
evpn df-election preference non-revertive
By default, non-revertive mode is disabled for preference-based DF election.

Setting the DF election delay

About this task

The DF election can be triggered by site-facing interface status changes, redundant PE membership changes, and interface ESI changes. To prevent frequent DF elections from degrading network performance, set the DF election delay. The DF election delay defines the minimum interval allowed between two DF elections.

Procedure

1. Enter system view.
system-view
2. Set the DF election delay.
evpn multihoming timer df-delay *delay-value*
By default, the DF election delay is 3 seconds.

Setting the advertisement delay timer for Ethernet auto-discovery routes

About this task

The advertisement delay timer for Ethernet auto-discovery routes helps reduce the traffic loss caused by a PE reboot at a multihomed EVPN VPLS network site.

At a multihomed EVPN VPLS network site, CE 1 is dualhomed to PE 1 and PE 2 through an aggregate link or smart trunk, and PE 3 is at a remote site. PE 1 forwards all traffic sent from CE 1 to the remote site, and PE 3 forwards the traffic that the remote site sends to CE 1 to both PE 1 and PE 2. When PE 1 reboots, it advertises Ethernet auto-discovery routes that carry next hop information to PE 3. If PE 3 has not received the MAC/IP advertisement routes advertised by PE 2 when receiving

the Ethernet auto-discovery routes, it will forward traffic to both PE 1 and PE 2. In this situation, PE 1 does not have MAC address entries for CE 1 and drops the traffic.

To resolve this issue, set the advertisement delay timer for Ethernet auto-discovery routes on the CE-facing interface of PE 1. This timer allows PE 3 to receive the MAC/IP advertisement routes advertised by PE 2 before the Ethernet auto-discovery routes advertised by PE 1 and update its MAC address table timely.

Procedure

1. Enter system view.
system-view
2. Enable interface view.
interface *interface-type interface-number*
3. Set the advertisement delay timer for Ethernet auto-discovery routes.
evpn timer ad-delay *delay-time*
By default, advertisement of Ethernet auto-discovery routes is not delayed.

Configuring local FRR for EVPN VPLS

About this task

Local fast reroute (FRR) enables two PEs at a multihomed EVPN VPLS network site to set up a PW between them. This feature helps reduce the traffic loss caused by AC failure.

Restrictions and guidelines

On an EVPN instance, EVPN instance-specific local FRR configuration takes precedence over global local FRR configuration.

If you have executed the **evpn frr local enable** command on an EVPN instance, the **undo evpn multihoming vpls-frr local** command does not disable local FRR for the EVPN instance.

Perform this task on redundant PEs at a multihomed EVPN VPLS network site.

Enabling local FRR globally

1. Enter system view.
system-view
2. Enable local FRR globally for EVPN VPLS.
evpn multihoming vpls-frr local
By default, local FRR is disabled globally for EVPN VPLS.

Configuring local FRR on an EVPN instance created in VSI view

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enter VSI EVPN instance view.
evpn encapsulation mpls
4. Configure local FRR on the EVPN instance.
evpn frr local { **disable** | **enable** }

By default, an EVPN instance uses the global local FRR configuration of EVPN VPLS.

Generating MAC address entries for received MAC/IP advertisement routes

About this task

This task helps reduce the traffic loss caused by AC failure at a dualhomed EVPN VPLS network site.

At a multihomed EVPN VPLS network site, CE 1 is dualhomed to PE 1 and PE 2 through an aggregate link or smart trunk, and PE 3 is at a remote site. PE 1 forwards all traffic sent from CE 1 to the remote site, and PE 3 forwards the traffic that the remote site sends to CE 1 to both PE 1 and PE 2. When the AC on PE 1 fails, PE 1 withdraws the MAC/IP advertisement routes advertised to PE 2 and PE 3. In this situation, PE 3 does not have MAC address entries for CE 1 until PE 2 learns MAC address entries for CE 1 and advertises them to PE 3. As a result, traffic interruption occurs.

To resolve this issue, perform this task on PE 2. When receiving the MAC/IP advertisement routes advertised by PE 1, PE 2 generates MAC address entries for the routes and advertises the entries to PE 3. PE 3 can use those MAC address entries to forward traffic to CE 1 when the AC on PE 1 fails.

Prerequisites

You must enable FRR for EVPN VPLS before you perform this task.

Procedure

1. Enter system view.
system-view
2. Enable the device to generate MAC address entries for received MAC/IP advertisement routes.
evpn multihoming re-originated mac
By default, the device does not generate MAC address entries for received MAC/IP advertisement routes.

Enabling VSIs to ignore the state of ACs

About this task

This task helps reduce the traffic loss caused by AC failure at a multihomed EVPN VPLS network site that uses single-active redundancy mode.

At a multihomed EVPN VPLS network site that uses single-active redundancy mode, CE 1 is dualhomed to PE 1 and PE 2 through a smart trunk. PE 1 is the primary PE, and PE 2 is the secondary PE. When the AC on PE 1 fails, PE 1 and PE 2 act as follows:

- PE 1 withdraws advertised Ethernet auto-discovery routes.
- PE 2 brings up its AC and advertises Ethernet auto-discovery routes to remote PEs.

The remote PEs switch traffic to the paths to PE 2 only after receiving the Ethernet auto-discovery routes advertised by PE 2, and traffic loss occurs during path switchover. To resolve this issue, enable VSIs to ignore the state of ACs on PE 2. This feature allows PE 2 to advertise Ethernet auto-discovery routes to remote PEs regardless of the state of ACs and speeds up path switchover when the AC on PE 1 fails.

Restrictions and guidelines for AC state ignore configuration

On a VSI, VSI-specific AC state ignore configuration takes precedence over global AC state ignore configuration.

If you have executed the **ignore-ac-state enable** command on a VSI, the **undo l2vpn ignore-ac-state** command does not disable the VSI from ignoring the state of ACs.

Perform this task together with the feature of generating MAC address entries for received MAC/IP advertisement routes.

Enabling VSIs to ignore the state of ACs globally

1. Enter system view.
system-view
2. Enable VSIs to ignore the state of ACs globally.
l2vpn ignore-ac-state
By default, VSIs does not ignore the state of ACs.

Configuring a VSI to ignore the state of ACs

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enable a VSI to ignore the state of ACs or disable a VSI from ignoring the state of ACs.
ignore-ac-state { **enable** | **disable** }
By default, a VSI uses the global AC state ignore configuration.

Disabling advertisement of EVPN multihoming routes

About this task

EVPN multihoming routes include Ethernet auto-discovery routes and Ethernet segment routes.

In a multihomed EVPN network, perform this task on a redundant PE before you reboot it. This operation allows other PEs to refresh their EVPN routing table to prevent traffic interruption caused by the reboot.

Procedure

1. Enter system view.
system-view
2. Disable advertisement of EVPN multihoming routes and withdraw the EVPN multihoming routes that have been advertised to remote sites.
evpn multihoming advertise disable
By default, the device advertises EVPN multihoming routes.

Ignoring the Ethernet tag on advertisement of Ethernet auto-discovery and MAC/IP advertisement routes

About this task

Perform this task on the redundant PEs at a dualhomed site.

This task enables the device to perform the following operations:

- Withdraw the Ethernet auto-discovery routes and MAC/IP advertisement routes that have been advertised.
- Set the Ethernet tag to 0 for the Ethernet auto-discovery routes and MAC/IP advertisement routes and re-advertise them.

After you configure ESIs for ACs on the redundant PEs at a dualhomed site, the PEs carry Ethernet tags in Ethernet auto-discovery and MAC/IP advertisement routes advertised to remote sites. If the remote peers are unable to identify Ethernet tags, you must perform this task on the redundant PEs to enable communication with the peers.

Restrictions and guidelines

After you assign an ESI to a Layer 3 main interface, its subinterfaces inherit the ESI if they do not have one. In addition, you must map two subinterfaces to different VSIs if the subinterfaces have the same ESI.

Procedure

1. Enter system view.

system-view

2. Enable the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes.

evpn multihoming advertise ignore-ethernet-tag

By default, the device advertises Ethernet auto-discovery routes and MAC/IP advertisement routes that carry Ethernet tags.

Enabling the device to monitor the BGP peer status of another local edge device

About this task

Perform this task on the CE-facing interfaces of the edge devices multihomed to a site to prevent device reboots from causing inter-site forwarding failure.

This task excludes unavailable edge devices from DF election at a multihomed site. After an edge device recovers from failure and brings up its CE-facing interface, it starts the advertisement delay timer for Ethernet segment routes and checks the status of the BGP peer specified in the **evpn track peer** command. If the BGP peer comes up before the timer expires, the edge device advertises Ethernet segment routes to the peer. If the BGP peer is still down when the timer expires, the edge device does not advertise Ethernet segment routes to the peer. The edge devices then perform DF election based on the Ethernet segment routes they have received.

Procedure

1. Enter system view.

system-view

2. Enter interface view.

- Enter Layer 2 Ethernet interface view.

interface *interface-type interface-number*

- Enter Layer 2 aggregate interface view.

interface bridge-aggregation *interface-number*

- Enter Layer 3 Ethernet interface view.

interface *interface-type interface-number*

- Enter Layer 3 aggregate interface view.

interface route-aggregation *interface-number*

3. Enable the device to monitor the BGP peer status of another local edge device.

evpn track peer *peer-address*

By default, the device does not monitor the BGP peer status of the other edge devices at a multihomed site.

4. Set the advertisement delay timer for Ethernet segment routes.

evpn timer es-delay *delay-time*

By default, advertisement of Ethernet segment routes is not delayed.

Managing remote MAC address entries and remote ARP learning

Disabling MAC address advertisement

About this task

The MAC information and ARP information advertised by the PE overlap. To avoid duplication, disable MAC address advertisement and withdraw the MAC addresses advertised to remote PEs.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enter VSI EVPN instance view.
evpn encapsulation mpls
4. Disable MAC address advertisement and withdraw advertised MAC addresses.
mac-advertising disable
By default, MAC address advertisement is enabled.

Disabling learning of MAC addresses from ARP information

About this task

The MAC information and ARP information advertised by a remote PE overlap. To avoid duplication, disable the learning of MAC addresses from ARP information. EVPN will learn remote MAC addresses only from the MAC information advertised from remote sites.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enter VSI EVPN instance view.

evpn encapsulation mpls

4. Disable the EVPN instance from learning MAC addresses from ARP information.

arp mac-learning disable

By default, an EVPN instance learns MAC addresses from ARP information.

Disabling ARP information advertisement

About this task

In an EVPN VPLS network, you can disable ARP information advertisement for an EVPN instance to save resources if all user terminals in the EVPN instance are attached to one PE. The EVPN instance will stop advertising ARP information through MAC/IP advertisement routes and withdraw advertised ARP information.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enter VSI EVPN instance view.
evpn encapsulation mpls
4. Disable ARP information advertisement for the EVPN instance.
arp-advertising disable
By default, ARP information advertisement is enabled for an EVPN instance.

Enabling EVPN E-tree

About this task

Use EVPN E-tree to isolate traffic between ACs based on the AC roles. This feature can better control AC access and improve security.

Restrictions and guidelines

Inter-site EVPN E-tree controls communication between local ACs and remote ACs. You do not need to enable this feature if you want to control communication between local ACs.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enter VSI EVPN instance view.
evpn encapsulation mpls
4. Enable inter-site EVPN E-tree.
e-tree enable
By default, inter-site EVPN E-tree is disabled.
5. Return to system view.
quit

quit

6. Execute the following commands to configure a Layer 3 interface as a leaf AC:
 - a. Enter Layer 3 interface view.
interface *interface-type interface-number*
 - b. Configure the AC as a leaf AC.
xconnect vsi *vsi-name leaf*
If you do not specify the **leaf** keyword for an AC, the AC acts as a root AC.
7. Execute the following commands to configure an Ethernet service instance as a leaf AC:
 - a. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.
interface *interface-type interface-number*
 - b. Enter Ethernet service instance view.
service-instance *instance-id*
 - c. Configure the AC as a leaf AC.
xconnect vsi *vsi-name leaf*
If you do not specify the **leaf** keyword for an AC, the AC acts as a root AC.

Confining floods to the local site

About this task

By default, the PE floods broadcast, unknown unicast, and unknown multicast frames received from the local site to the following interfaces in the frame's VSI:

- All site-facing interfaces except for the incoming interface.
- All PWs.

To confine a kind of flood traffic to the site-facing interfaces, disable flooding for that kind of flood traffic on the VSI. The VSI will not flood the corresponding frames to PWs.

To exclude a remote MAC address from the flood suppression done by using this feature, enable selective flood for the MAC address. The PE will flood the frames destined for the MAC address to remote sites.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Disable flooding for the VSI.
flooding disable
By default, flooding is enabled for a VSI.
4. (Optional.) Enable selective flood for a MAC address.
selective-flooding mac-address *mac-address*

Enabling ARP flood suppression

About this task

Use ARP flood suppression to reduce ARP request broadcasts.

The aging timer is fixed at 25 minutes for ARP flood suppression entries. If the **flooding disable** command is configured, set the MAC aging timer to a higher value than the aging timer for ARP flood suppression entries on all PEs. This setting prevents the traffic blackhole that occurs when a MAC address entry ages out before its ARP flood suppression entry ages out. To set the MAC aging timer, use the **mac-address timer** command.

Procedure

1. Enter system view.
system-view
2. Enter VSI view.
vsi *vsi-name*
3. Enable ARP flood suppression.
arp suppression enable
By default, ARP flood suppression is disabled.

Enabling packet statistics for an AC

Restrictions and guidelines for AC packet statistics

For the **ac statistics enable** command to take effect on a Layer 3 interface, you must map the Layer 3 interface to a VSI. When you modify the VSI mapping, the packet statistics of the interface are cleared. To display the statistics, use the **display l2vpn interface verbose** command.

To clear packet statistics for ACs, use the **reset l2vpn statistics ac** command.

Enabling packet statistics for a Layer 3 interface

1. Enter system view.
system-view
2. Enter interface view.
 - Enter Layer 3 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.
interface route-aggregation *interface-number*
3. Enable packet statistics for the Layer 3 interface.
ac statistics enable
By default, the packet statistics feature is disabled for Layer 3 interfaces that act as ACs.

Enabling SNMP notifications for L2VPN PWs

About this task

This feature enables L2VPN to generate SNMP notifications when PW deletions, PW switchovers, or PW status changes occur. For L2VPN event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Procedure

1. Enter system view.

system-view

2. Enable SNMP notifications for L2VPN PWs.

snmp-agent trap enable l2vpn [**pw-delete** | **pw-switch** | **pw-up-down**] *

By default, SNMP notifications for L2VPN PWs are disabled.

For more information about this command, see VPLS commands in *MPLS Command Reference*.

Display and maintenance commands for EVPN VPLS

Execute **display** commands in any view and **reset** commands in user view.

For more information about the following BGP commands, see *Layer 3—IP Routing Command Reference*:

- **display bgp group.**
- **display bgp peer.**
- **display bgp update-group.**

Task	Command
Display BGP peer group information.	display bgp [instance <i>instance-name</i>] group l2vpn evpn [group-name <i>group-name</i>]
Display BGP EVPN routes.	display bgp [instance <i>instance-name</i>] l2vpn evpn [peer { <i>ipv4-address</i> <i>ipv6-address</i> } { advertised-routes received-routes } [statistics] [route-distinguisher <i>route-distinguisher</i> route-type { auto-discovery es imet mac-ip }] * [{ <i>evpn-route</i> <i>route-length</i> <i>evpn-prefix</i> } [advertise-info] <i>ipv4-address</i> <i>ipv6-address</i> <i>mac-address</i>] statistics]
Display BGP peer or peer group information.	display bgp [instance <i>instance-name</i>] peer l2vpn evpn [<i>ipv4-address</i> <i>mask-length</i> { <i>ipv4-address</i> group-name <i>group-name</i> } log-info [<i>ipv4-address</i>] verbose]
Display information about BGP update groups.	display bgp [instance <i>instance-name</i>] update-group l2vpn evpn [<i>ipv4-address</i>]
Display information about peers that are automatically discovered through BGP.	display evpn auto-discovery { { imet mac-ip } [mpls] [peer <i>ip-address</i>] [vsi <i>vsi-name</i>] macip-prefix [nexthop <i>next-hop</i>] [count] }
Display EVPN ES information.	display evpn es { local [count [vsi <i>vsi-name</i>] [<i>esi</i> <i>esi-id</i>] [verbose]] remote [vsi <i>vsi-name</i>] [<i>esi</i> <i>esi-id</i>] [nexthop <i>next-hop</i>] [verbose] }
Display EVPN ARP entries.	display evpn route arp [local remote] [public-instance vpn-instance <i>vpn-instance-name</i>] [count]
Display ARP flood suppression entries.	display evpn route arp suppression [mpls vxlan] [local remote] [vsi <i>vsi-name</i>] [count]
Display EVPN MAC address entries.	display evpn route mac [mpls vxlan] [local

Task	Command
	remote [vsi <i>vsi-name</i>] [count]
Display the routing table for a VPN instance.	display evpn routing-table { public-instance vpn-instance <i>vpn-instance-name</i> } [count]
Display EVPN instance information.	display evpn instance [vsi <i>vsi-name</i>] [verbose]
Display site-facing interfaces excluded from traffic forwarding by split horizon.	In standalone mode: display l2vpn forwarding evpn split-horizon { ac interface <i>interface-type interface-number</i> tunnel <i>tunnel-number</i> } In IRF mode: display l2vpn forwarding evpn split-horizon { ac interface <i>interface-type interface-number</i> tunnel <i>tunnel-number</i> } [slot <i>slot-number</i>]
Display information about EVPN VPLS forwarding.	In standalone mode: display l2vpn forwarding evpn vsi [name <i>vsi-name</i>] [verbose] In IRF mode: display l2vpn forwarding evpn vsi [name <i>vsi-name</i>] [slot <i>slot-number</i>] [verbose]

Command reference

arp-advertising disable

Use **arp-advertising disable** to disable ARP information advertisement for an EVPN instance.

Use **undo arp-advertising disable** to restore the default.

Syntax

arp-advertising disable

undo arp-advertising disable

Default

ARP information advertisement is enabled for an EVPN instance.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

In an EVPN network with distributed gateways, you can disable ARP information advertisement for a VXLAN to save resources if all its user terminals use the same EVPN gateway device. The EVPN instance of the VXLAN will stop advertising ARP information through MAC/IP advertisement routes and withdraw advertised ARP information. When ARP information advertisement is disabled, user terminals in other VXLANs still can communicate with that VXLAN through IP prefix advertisement routes.

Examples

Disable ARP information advertisement for an EVPN instance.

```
<Sysname> system-view
[Sysname] vsi aaa
[Sysname-vsi-aaa] evpn encapsulation vxlan
[Sysname-vsi-aaa-evpn-vxlan] arp-advertising disable
```

display evpn es

Use **display evpn es** to display EVPN ES information.

Syntax

```
display evpn es { local [ count | [ vsi vsi-name | xconnect-group group-name ] [ esi esi-id ] [ verbose ] ] | remote [ vsi vsi-name | xconnect-group group-name ] [ esi esi-id ] [ nexthop next-hop ] [ verbose ] }
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

local: Specifies local ES information.

count: Displays the number of local ESs.

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays ES information about all VSIs.

xconnect-group *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a cross-connect group, this command displays EVPN local or remote ES information about all cross-connect groups.

esi *esi-id*: Specifies an ES by its ESI in XXXX.XXXX.XXXX.XXXX.XXXX format. Each X represents a hexadecimal digit. The ESI must begin with **00** and cannot be all zeros. If you do not specify this option, the command displays information about all ESs.

verbose: Displays detailed ES information. If you do not specify this keyword, the command displays brief ES information.

remote: Specifies remote ES information.

nexthop *next-hop*: Specifies a next hop. If you do not specify this option, the command displays ES information received from all next hops.

Examples

Display the number of local ESs.

```
<Sysname> display evpn es local count
Total number of ES entries: 1
```

Display brief information about local ESs of VSI **vpna** for EVPN VPLS.

```
<Sysname> display evpn es local vsi vpna
Redundancy mode: A - All-active, S - Single-active
```

```
VSI name : vpna
```

```

EVPN instance: -
ESI                Tag ID      DF address      Mode  State ESI label
0001.0002.0002.0002.0002  -        1.1.1.1        A    Up    1000
0001.0002.0003.0004.0005  -        1.1.1.1        A    Up    1001
0003.0003.0003.0003.0003  2        2.2.2.2        A    Up    1002

```

Display brief information about local ESs of VSI **vpna** for EVPN VPLS over SRv6.

```
<Sysname> display evpn es local vsi vpna
```

Redundancy mode: A - All-active, S - Single-active

VSI name : vpna

EVPN instance: -

```

ESI      : 0001.0001.0001.0001.0001
Tag ID   : -
DF address : 1.1.1.1
Mode     : A
State    : Down
Argument : ::1

```

Display brief information about local ESs of cross-connect group **vpna** for EVPN VPWS.

```
<Sysname> display evpn es local xconnect-group vpna
```

Redundancy mode: A - All-active, S - Single-active

Xconnect group name: vpna

```

ESI                Tag ID      DF address      Mode  State ESI label
0001.0002.0002.0002.0002  -        1.1.1.1        A    Up    -
0001.0002.0003.0004.0005  -        1.1.1.1        A    Up    -
0003.0003.0003.0003.0003  2        2.2.2.2        A    Up    -

```

Display brief information about local ESs of cross-connect group **vpna** for EVPN VPLS over SRv6.

```
<Sysname> display evpn es local xconnect-group vpna
```

Redundancy mode: A - All-active, S - Single-active

Xconnect-group name : vpna

```

ESI      : 0001.0001.0001.0001.0001
Tag ID   : -
DF address : 1.1.1.1
Mode     : A
State    : Up
Argument : -

```

Table 88 Command output

Field	Description
EVPN instance	EVPN instance name. This field displays a hyphen (-) for a VSI EVPN instance.
Xconnect group name	Cross-connect group name.
Tag ID	Ethernet tag ID.
DF address	Router ID of the VTEP or PE elected as the DF.
Mode	Redundancy mode of the ES: A—All-active mode.

Field	Description
	S—Single-active mode.
State	State of the ES: Up. Down.
ESI label	ESI label. For EVPN VPWS and EVPN VXLAN, this field is invalid and displays a hyphen (-).
Argument	Argument that identifies a leaf AC. E-tree isolates traffic among leaf ACs based on arguments in an EVPN VPLS over SRv6 network. This field displays a hyphen (-) if no argument exists.

Display detailed information about local ESs of all VSIs.

```
<Sysname> display evpn es local verbose
```

```
VSI name : v1
```

```
EVPN instance: -
```

```
ESI : 0003.0003.0003.0003.0003
```

```
Interface : GigabitEthernet1/0/1
```

```
Redundancy mode : All-active
```

```
State : Up
```

```
AD-delay remaining time : 10
```

```
ACs :
```

Link ID	Service instance ID	Tag ID	DF address	ESI label
0	1	1	1.1.1.1	1001
1	3	3	3.3.3.3	1002
2	10	10	2.2.2.2	1003

```
VSI name : v2
```

```
EVPN instance: -
```

```
ESI : 0004.0004.0004.0004.0004
```

```
Interface : -
```

```
Redundancy mode : All-active
```

```
State : Up
```

```
AD-delay remaining time : 10
```

```
UPWs :
```

Link ID	Tag ID	DF address	ESI label
0	1	1.1.1.1	1004

```
VSI name : vpna
```

```
EVPN instance: -
```

```
ESI : 0001.0002.0002.0002.0002
```

```
Interface : GigabitEthernet1/0/2
```

```
Redundancy mode : All-active
```

```
State : Up
```

```
AD-delay remaining time : 10
```

```
ACs :
```

Link ID	Service instance ID	Tag ID	DF address	ESI label
1	-	-	1.1.1.1	-

```

VSI name : vpnb
EVPN instance: -
  ESI : 0001.0001.0001.0001.0001
  Interface : GigabitEthernet1/0/3
  Redundancy mode : All-active
  State : Down
  ACs :
    Link ID : 0
    Service instance ID : -
    Tag ID : -
    DF address : 1.1.1.1
    Argument : ::1

```

```

Xconnect group name : vpna
  Connection name : aa
  ESI : 0003.0003.0003.0003.0003
  AC : GE1/0/5 srv1
  Redundancy mode : All-active
  State : Up
  Link ID : 0
  Tag ID : 10
  DF address : 1.1.1.1

```

```

Xconnect group name : vpnd
  Connection name : dd
  ESI : 0006.0006.0006.0006.0006
  Redundancy mode : All-active
  State : Up
  UPW Link ID : 0
  Tag ID : 10
  DF address : 1.1.1.1

```

Table 89 Command output

Field	Description
EVPN instance	EVPN instance name. This field displays a hyphen (-) for a VSI EVPN instance.
Xconnect group name	Cross-connect group name.
Connection name	Cross-connect name.
AC	AC name. This field displays a Layer 3 interface name
Redundancy mode	Redundancy mode of the ES: A—All-active mode. S—Single-active mode.
State	State of the ES: Up. Down. If the ES is not manually assigned an ESI, a hyphen (-) is displayed.

Field	Description
AD-delay remaining time	Remaining time of the advertisement delay timer for Ethernet auto-discovery routes, in seconds.
ACs	The VSI's ACs on the ES.
UPWs	The VSI's UPWs on the ES.
Link ID	The AC's link ID on the VSI.
Service instance ID	Ethernet service instance ID.
Tag ID	Ethernet tag ID.
DF address	Router ID of the VTEP or PE elected as the DF. If the device is not the DF of an AC, a hyphen (-) is displayed.
ESI label	ESI label. For EVPN VPWS and EVPN VXLAN, this field is invalid and displays a hyphen (-).
Argument	Argument that identifies a leaf AC. E-tree isolates traffic among leaf ACs based on arguments in an EVPN VPLS over SRv6 network. This field displays a hyphen (-) if no argument exists.
UPW link ID	The UPW's link ID on the VSI.

Display information about remote ESs of all VSIs.

```
<Sysname> display evpn es remote
```

Control Flags: P - Primary, B - Backup, C - Control word

VSI name : vpna

EVPN instance: -

ESI : 0001.0000.0000.0000.0001

Ethernet segment routes :

1.1.1.1

3.3.3.3

A-D per ES routes :

Peer IP Remote Redundancy mode

1.1.1.1 All-active

3.3.3.3 All-active

A-D per EVI routes :

Tag ID Peer IP

- 1.1.1.1

- 3.3.3.3

ESI : 0001.0002.0003.0004.0005

Ethernet segment routes :

1.1.1.1

A-D per ES routes :

Peer IP Remote Redundancy mode

1.1.1.1 All-active

A-D per EVI routes :

Tag ID Peer IP

- 1.1.1.1

```

Xconnect group name : a
  ESI : 0001.0000.0000.0000.0001
  Ethernet segment routes :
    123.123.123.123
    3.3.3.3
  A-D per ES routes :
    Peer IP Remote Redundancy mode
    123.123.123.123 All-active
    3.3.3.3 All-active
  A-D per EVI routes :
    Tag ID Peer IP Control Flags
    2 3.3.3.3 P
    4 123.123.123.123 PC

```

Display detailed information about remote ESs.

```

<Sysname> display evpn es remote
Control Flags: P - Primary, B - Backup, C - Control word

```

```

VSI name : vpna
EVPN instance: -
  ESI : 0001.0001.0001.0001.0001
  A-D per ES routes :
    Peer IP : 2::2
    Remote Redundancy mode: All-active
    Argument : ::1
  A-D per EVI routes :
    Tag ID : 1
    Peer IP : 2::2

```

```

Xconnect group name : vpna
  ESI : 0001.0001.0001.0001.0001
  Ethernet segment routes :
    2::2
  A-D per ES routes :
    Peer IP : 2::2
    Remote Redundancy mode: All-active
  A-D per EVI routes :
    Tag ID : 1
    Control Flags : P
    Peer IP : 2::2

```

Display remote ES information received from next hop 3.3.3.3 for VSI vpna.

```

<Sysname> display evpn es remote vsi vpna nexthop 3.3.3.3

```

```

VSI name : vpna
EVPN instance: -
  ESI : 0001.0000.0000.0000.0001
  Redundancy mode : All-active
  Ethernet segment routes :
    3.3.3.3

```

```

A-D per ES routes      :
  3.3.3.3
A-D per EVI routes     :
  Tag ID      Peer IP
  -           3.3.3.3

```

Table 90 Command output

Field	Description
EVPN instance	EVPN instance name. This field displays a hyphen (-) for a VSI EVPN instance.
Xconnect group name	Cross-connect group name.
Argument	Argument that identifies a leaf AC. E-tree isolates traffic among leaf ACs based on arguments in an EVPN VPLS over SRv6 network. This field displays a hyphen (-) if no argument exists.
Ethernet segment routes	Ethernet segment routes for the ES.
A-D per Ethernet segment routes	A-D per Ethernet segment routes for the ES.
A-D per EVI routes	A-D per EVI routes for the ES.
Tag ID	Ethernet tag ID.
Peer IP	IP address of the remote peer.
Remote Redundancy mode	Redundancy mode of the remote ES: • All-active. • Single-active.
Control Flags	Layer 2 attributes control flags of the remote route: • P—Primary flag. • B—Backup flag. • C—Control word flag.

display evpn df-election

Use **display evpn df-election** to display DF election information.

Syntax

display evpn df-election [**vsi** *vsi-name* | **xconnect-group** *group-name*] [**esi** *esi-id*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

xconnect-group *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters.

esi esi-id: Specifies an ES by its ESI in XXXX.XXXX.XXXX.XXXX.XXXX format. Each X represents a hexadecimal digit. The ESI must begin with **00** and cannot be all zeros. If you do not specify this option, the command displays information about all ESs.

Usage guidelines

If you do not specify a VSI or cross-connect group, this command displays DF election information about all VSIs and cross-connect groups.

Examples

Display DF election information about all VSIs and cross-connect groups.

```
<Sysname> display evpn df-election
VSI name: 1
  ESI : 0021.1001.1001.1001.1002
  Interface : GigabitEthernet1/0/1
  Service instance ID : 1000
  Link ID      : 1
  Ethernet tag ID : 12
  DF state     : DF
  FSM          : DF_DONE
  Number of member devices : 2
    Originating IP  DF state  Algorithm  Preference  Capability
    100.100.100.100  DF      Preference  65535      DP
    100.100.100.200  BDF     Preference  200        DP

  ESI : 0002.0002.0002.0002.0002
  Interface : GigabitEthernet1/0/2
  Link ID      : 0
  Ethernet tag ID : -
  DF state     : -
  FSM          : DF_CALC
  Number of member devices : 2
    Originating IP  DF state  Algorithm  Preference  Capability
    1.1.1.1         -          Preference  32767      -
    2.2.2.2         -          Preference  32767      -

Xconnect-group name : 1
Connection name : 1
  ESI : 0001.0001.0001.0001.0001
  Interface : GigabitEthernet1/0/3
  Link ID      : 1
  Ethernet tag ID : -
  DF state     : -
  FSM          : DF_CALC
  Number of member devices : 1
    Originating IP  DF state  Algorithm  Preference  Capability
    2.2.2.2         -          Preference  32767      -
```

Table 91 Command output

Field	Description
Link ID	The AC's link ID on the VSI.

Field	Description
DF state	DF election result: BDF—The device is a BDF. DF—The device is the DF. If DF election has not finished, this field displays a hyphen (-).
FSM	State of the finite state machine for DF election: INIT—Initializing. DF_WAIT—The DF election delay has not timed out. DF_CALC—DF election is in progress. DF_DONE—DF election has finished.
Originating IP	IP address of the member device that participates in DF election.
DF state	DF election result: BDF—The member device is a BDF. DF—The member device is the DF. If DF election has not finished, this field displays a hyphen (-).
Algorithm	Algorithm used in DF election: modulus—VLAN tag-based algorithm. Preference—Preference-based algorithm.
Preference	DF election preference.
Capability	Supported DF election capabilities. DP represents non-revertive mode. If no capability is supported, this field displays a hyphen (-).

display evpn instance

Use **display evpn instance** to display EVPN instance information.

Syntax

display evpn instance [**vsi** *vsi-name* | **xconnect-group** *group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

vsi *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters.

xconnect-group *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters.

verbose: Displays detailed EVPN instance information. If you do not specify this keyword, the command displays brief EVPN instance information.

Usage guidelines

If you do not specify any parameters, this command displays information about all EVPN instances.

Examples

Display brief information about all EVPN instances.

```
<Sysname> disp evpn instance
```

Total number of EVPN instances: 4

EVPN name	EVPN index
a	0x0
aaa	0x1
bbb	0x2
ccc	0x3

Display detailed information about all EVPN instances.

<Sysname> display evpn instance verbose

VSI Name: aaa

EVPN index	: 0x1
Encapsulation	: VXLAN
Route distinguisher	: -
Export VPN targets	: -
Import VPN targets	: -
MAC advertisement	: Enabled
ARP-based MAC learning	: Enabled
VXLAN ID	: -

VSI Name: bbb

EVPN index	: 0x2
Encapsulation	: SRv6
Route distinguisher	: -
Export VPN targets	: -
Import VPN targets	: -
MAC advertisement	: Enabled
ARP-based MAC learning	: Enabled
Dt2u SID	: -
Dt2ul SID	: -
Dt2m SID	: -
Dt2uLocatorName	: -
Dt2ulLocatorName	: -
Dt2mLocatorName	: -
E-Tree	: Disabled
Best-Effort	: Disabled
Traffic-Engineering	: Disabled
Import Route Policy	: -
Export Route Policy	: -

VSI Name: vpna

EVPN index	: 0x0
Encapsulation	: MPLS
Route distinguisher	: 1:1
Export VPN targets	: 1:1
Import VPN targets	: 1:1
MAC advertisement	: Enabled
ARP-based MAC learning	: Enabled


```

MPLS label           : 24128
IMET MPLS label      : 24127
Tunnel policy        : -
PW class             : -
Control Word         : Disabled
E-Tree               : Disabled
PW type              : VLAN
Sequencing           : -
Import Route Policy  : -
Export Route Policy  : -

```

Table 92 Command output

Field	Description
Encapsulation	EVPN encapsulation type: • VXLAN. • MPLS. • SRv6.
MAC advertisement	Status of MAC address advertisement: • Enabled. • Disabled.
ARP-based MAC learning	Whether EVPN learns MAC addresses from ARP information: • Enabled. • Disabled.
MPLS label	MPLS label in MAC/IP advertisement routes.
IMET MPLS label	MPLS label in IMET routes.
Tunnel policy	Tunnel policy used by the EVPN instance.
PW class	PW class used by the EVPN instance.
Control word	Status of the control word feature: • Enabled. • Disabled.
E-Tree	Status of EVPN E-tree: • Enabled. • Disabled.
PW type	PW type: • Ethernet. • VLAN.
Sequencing	Sequencing on the PW. The value is Both . A hyphen (-) in this field indicates that sequencing is disabled on the PW.
Flow label	Flow label capability: • Both—Flow label sending and receiving capabilities. • Send—Flow label sending capability. • Recv—Flow label receiving capability. This field displays a hyphen (-) if the flow label feature is disabled.
Dt2u SID	SRv6 SID used for unicast forwarding in the EVPN VPLS over SRv6 network. The values in parentheses are the length of each segment in the SID, which are the locator length, dynamic opcode length, static

Field	Description
	opcode length, and argument length in sequence. The total length of those segments is 128.
Dt2ul SID	SRv6 SID used for unicast forwarding over the bypass tunnel at the multihomed EVPN VPLS over SRv6 site. The values in parentheses are the length of each segment in the SID, which are the locator length, dynamic opcode length, static opcode length, and argument length in sequence. The total length of those segments is 128.
Dt2m SID	SRv6 SID used for multicast forwarding in the EVPN VPLS over SRv6 network. The values in parentheses are the length of each segment in the SID, which are the locator length, dynamic opcode length, static opcode length, and argument length in sequence. The total length of those segments is 128.
Dt2uLocatorName	Locator name used for requesting the DT2U SID. If dynamic SID assignment is disabled, this field displays auto-sid-disable .
Dt2ulLocatorName	Locator name used for requesting the DT2UL SID. If dynamic SID assignment is disabled, this field displays auto-sid-disable .
Dt2mLocatorName	Locator name used for requesting the DT2M SID. If dynamic SID assignment is disabled, this field displays auto-sid-disable .
Best-Effort	Whether SID-route-recursion is enabled: • Enabled. • Disabled.
Import routing policy	Importing routing policy used by the EVPN instance. If the EVPN instance does not have an import routing policy, this field displays a hyphen (-). This field is available only when the encapsulation type is SRv6.
Export routing policy	Exporting routing policy used by the EVPN instance. If the EVPN instance does not have an export routing policy, this field displays a hyphen (-). This field is available only when the encapsulation type is SRv6.

Related commands

evpn encapsulation

vsi

display l2vpn forwarding evpn

Use **display l2vpn forwarding evpn** to display forwarding information of EVPN VPLS/VPWS and EVPN VPLS/VPWS over SRv6.

Syntax

In standalone mode:

display l2vpn forwarding evpn [**vsi** [**name** *vsi-name*] [**verbose**]]

In IRF mode:

display l2vpn forwarding evpn [**vsi** [**name** *vsi-name*] [**verbose**]] **slot** *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vsi: Specifies VSI forwarding information. If you do not specify this keyword, the command displays both VSI and cross-connect forwarding information about EVPN.

name *vsi-name*: Specifies a VSI by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command displays forwarding information about all VSIs.

verbose: Displays detailed forwarding information. If you do not specify this keyword, the command displays brief forwarding information.

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Examples

(In standalone mode.) Display brief forwarding information about all VSIs of EVPN VPLS.

```
<Sysname> display l2vpn forwarding evpn vsi
```

Total number of VSIs: 2

VSI name	VSI index
vpls1	0

(In IRF mode.) Display brief forwarding information about all VSIs of EVPN VPLS on slot 1.

```
<Sysname> display l2vpn forwarding evpn vsi slot 1
```

Total number of VSIs: 2

VSI name	VSI index
vpls1	0

(In standalone mode.) Display detailed forwarding information about all VSIs of EVPN VPLS.

```
<Sysname> display l2vpn forwarding evpn vsi verbose
```

VSI name: vpls1

VSI index	: 0
Encapsulation	: MPLS
MPLS label	: 1150
IMET MPLS label	: 1149
Control word	: enabled
PW type	: Ethernet
Sequencing	: Both
Flow label	: Both

(In IRF mode.) Display detailed forwarding information about all VSIs of EVPN VPLS on slot 1.

```
<Sysname> display l2vpn forwarding evpn vsi verbose slot 1
```

VSI name: vpls1

VSI index	: 0
Encapsulation	: MPLS
MPLS label	: 1150
IMET MPLS label	: 1149
Control word	: enabled
PW type	: Ethernet
Sequencing	: Both
Flow label	: Both

Table 93 Command output

Field	Description
Encapsulation	EVPN encapsulation type:

Field	Description
	• MPLS. • SRv6.
MPLS label	MPLS label in MAC/IP advertisement routes.
IMET MPLS label	MPLS label in IMET routes.
Control word	Status of the control word feature: • enabled. • disabled.
PW type	PW type: • Ethernet. • VLAN.
Sequencing	Sequencing on the PW. The value is Both . A hyphen (-) in this field indicates that sequencing is disabled on the PW.
Flow label	Flow label capability: • Both—Flow label sending and receiving capabilities. • Send—Flow label sending capability. • Recv—Flow label receiving capability. This field displays a hyphen (-) if the flow label feature is disabled.
Dt2u SID	SRv6 SID used for unicast forwarding.
Dt2ul SID	SRv6 SID used for unicast forwarding over the bypass tunnel at the multihomed site.
Dt2m SID	SRv6 SID used for multicast forwarding.

Related commands

evpn encapsulation

vsi

display l2vpn forwarding evpn split-horizon

Use **display l2vpn forwarding evpn split-horizon** to display site-facing interfaces excluded from traffic forwarding by split horizon.

Syntax

In standalone mode:

```
display l2vpn forwarding evpn split-horizon { ac interface interface-type interface-number
| ac interface interface-type interface-number service-instance instance-id | tunnel
tunnel-number | upw vsi vsi-name }
```

In IRF mode:

```
display l2vpn forwarding evpn split-horizon { ac interface interface-type interface-number
| ac interface interface-type interface-number service-instance instance-id | tunnel
tunnel-number | upw vsi vsi-name } [ slot slot-number
]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

ac interface *interface-type interface-number*: Specifies a Layer 3 interface by its type and number. These parameters apply to EVPN VPLS.

ac interface *interface-type interface-number service-instance instance-id*: Specifies an Ethernet service instance on a Layer 2 interface. The *interface-type interface-number* argument specifies the interface by its type and number. The *instance-id* argument specifies the Ethernet service instance by its ID in the range of 1 to 4096. These parameters apply to EVPN VPLS.

tunnel *tunnel-number*: Specifies a VXLAN tunnel interface number. The value range for the *tunnel-number* argument varies by device model. If you do not specify this option, the command displays all site-facing interfaces excluded from traffic forwarding by split horizon. This option applies to EVPN VXLAN.

upw vsi *vsi-name*: Specifies a VSI name, a case-sensitive string of 1 to 31 characters. If you specify a VSI, this command displays the SRv6 PWs or EVPN PWs excluded by split horizon from forwarding flood traffic received from LDP PWs or static PWs. This option applies to EVPN VPLS or EVPN VPLS over SRv6.

slot *slot-number*: Specifies an IRF member device by its member ID. (In IRF mode.)

Examples

Display site-facing interfaces excluded from traffic forwarding for Tunnel 0.

```
<Sysname> display l2vpn forwarding evpn split-horizon tunnel 0
Tunnel name: 0
  Total number of filtered interfaces: 2
  Filtered interfaces:
    GE1/0/1
    GE1/0/2
```

For EVPN VPLS, display site-facing interfaces excluded from traffic forwarding for AC GigabitEthernet 1/0/1.

```
<Sysname> display l2vpn forwarding evpn split-horizon ac interface gigabitethernet 1/0/1
Interface name   : GigabitEthernet1/0/1
AC link ID       : 0
Service instance ID : 100
PW count         : 2
VSI name         PW link ID      ESI label
vpna              8               775128
vpna              9               775128
```

For EVPN VPLS over SRv6, display site-facing interfaces excluded from traffic forwarding for AC GigabitEthernet 1/0/1.

```
<Sysname> display l2vpn forwarding evpn split-horizon ac interface gigabitethernet 1/0/1
Interface name   : GigabitEthernet1/0/1
AC link ID       : 0
Service instance ID : 100
SRv6 tunnel count : 2
VSI name         SRv6 link ID      Argument
vpna              0x8               ::1
vpna              0x9               ::1
```

For EVPN VPLS, display SRv6 PWs or EVPN PWs excluded by split horizon from forwarding flood traffic received from LDP PWs or static PWs for VSI **vpna**.

```
<Sysname> display l2vpn forwarding evpn split-horizon upw vsi vpna
UPW link ID           : 0
PW count              : 2
VSI name              PW link ID      Argument
vpna                  0x8             ::1
vpna                  0x9             ::1
```

For EVPN VPLS over SRv6, display SRv6 PWs or EVPN PWs excluded by split horizon from forwarding flood traffic received from LDP PWs or static PWs for VSI **vpna**.

```
<Sysname> display l2vpn forwarding evpn split-horizon upw vsi vpna
UPW link ID           : 0
SRv6 tunnel count     : 2
VSI name              SRv6 link ID    Argument
vpna                  0x8             ::1
vpna                  0x9             ::1
```

Table 94 Command output

Field	Description
Tunnel name	VXLAN tunnel interface name.
Argument	Argument that identifies a leaf AC. E-Tree isolates traffic among leaf ACs based on arguments in an EVPN VPLS over SRv6 network. This field displays a hyphen (-) if no argument exists.
Filtered interfaces	Site-facing interfaces that do not forward the flood traffic received from the VXLAN tunnel.

e-tree enable

Use **e-tree enable** to enable inter-site EVPN E-tree.

Use **undo e-tree enable** to disable inter-site EVPN E-tree.

Syntax

e-tree enable

undo e-tree enable

Default

Inter-site EVPN E-tree is disabled.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

In an EVPN VPLS or VPLS over SRv6 network, EVPN E-tree isolates unicast and flood traffic (broadcast, multicast, and unknown unicast) of ACs in the same EVPN instance based on the AC roles. With EVPN E-tree, the device isolates unicast and flood traffic of ACs in the same EVPN instance as follows:

- Leaf ACs can access root ACs.
- Leaf ACs cannot access each other.
- Root ACs can access each other and access leaf ACs.

Inter-site EVPN E-tree controls communication between local ACs and remote ACs. You do not need to enable this feature if you want to control communication between local ACs.

You cannot configure inter-site EVPN E-tree for both EVPN VPLS and EVPN VPLS over SRv6.

Examples

Enable inter-site EVPN E-tree.

```
<Sysname> system-view
[Sysname] vsi aaa
[Sysname-vsi-aaa] evpn encapsulation mpls
[Sysname-vsi-aaa-evpn-mpls] e-tree enable
```

evpn df-election algorithm (interface view)

Use **evpn df-election algorithm** to configure the DF election algorithm on an interface.

Use **undo evpn df-election algorithm** to restore the default.

Syntax

evpn df-election algorithm *algorithm*

undo evpn df-election algorithm

Default

The DF election algorithm specified in system view takes effect.

Views

Interface view

Predefined user roles

network-admin

Parameters

Algorithm: Specifies a DF election algorithm. The value of this argument can only be **preference**, which represents the preference-based algorithm.

Usage guidelines

At a multihomed EVPN network site, you can modify the DF election algorithm with this command to control the DF election result.

You can configure the DF election algorithm in system view and in interface view. The global DF election algorithm takes effect on all ESS, and the interface-specific DF election algorithm takes effect only on the ESS on an interface. The interface-specific DF election algorithm takes precedence over the global DF election algorithm.

Examples

Configure GigabitEthernet 1/0/1 to use the preference-based algorithm for DF election.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn df-election algorithm preference
```

Related commands

evpn df-election algorithm (system view)

evpn df-election preference

evpn df-election algorithm (system view)

Use **evpn df-election algorithm** to configure the DF election algorithm globally.

Use **undo evpn df-election algorithm** to restore the default.

Syntax

evpn df-election algorithm *algorithm*

undo evpn df-election algorithm

Default

The VLAN tag-based algorithm is used for DF election.

Views

System view

Predefined user roles

network-admin

Parameters

algorithm: Specifies a DF election algorithm. The value of this argument can only be **preference**, which represents the preference-based algorithm.

Usage guidelines

At a multihomed EVPN network site, you can modify the DF election algorithm with this command to control the DF election result.

You can configure the DF election algorithm in system view and in interface view. The global DF election algorithm takes effect on all ESS, and the interface-specific DF election algorithm takes effect only on the ESS on an interface. The interface-specific DF election algorithm takes precedence over the global DF election algorithm.

Examples

```
# Configure the global DF election algorithm as the preference-based algorithm.
```

```
<Sysname> system-view
```

```
[Sysname] evpn df-election algorithm preference
```

Related commands

evpn df-election algorithm (interface view)

evpn df-election preference

evpn df-election preference

Use **evpn df-election preference** to set the DF election preference.

Use **undo evpn df-election preference** to restore the default.

Syntax

evpn df-election preference *preference*

undo evpn df-election preference

Default

The DF election preference is 32767.

Views

Interface view

Predefined user roles

network-admin

Parameters

Preference: Sets the DF election preference in the range of 0 to 65535. The larger the value, the higher the preference.

Usage guidelines

Use this command to set the preference used in preference-based DF election. The device with higher preference will be elected as the DF.

The DF election preference takes effect after the **evpn df-election algorithm preference** command is executed in interface or system view.

Examples

```
# Set the DF election preference to 100.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn df-election preference 100
```

Related commands

evpn df-election algorithm (interface view)

evpn df-election algorithm (system view)

evpn df-election preference non-revertive

Use **evpn df-election preference non-revertive** to enable non-revertive mode for preference-based DF election.

Use **undo evpn df-election preference non-revertive** to disable non-revertive mode for preference-based DF election.

Syntax

evpn df-election preference non-revertive

undo evpn df-election preference non-revertive

Default

Non-revertive mode is disabled for preference-based DF election.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

Preference-based DF election selects the device with the highest preference as the DF. The BDF takes over the DF role if one of the following events occurs:

- The DF fails.
- The site-facing link on the DF fails.
- The DF election preference of the BDF is set to be higher than that of the DF.

When the original DF or its site-facing link recovers, or its preference is set to be higher than that of the new DF, the original DF will take over the DF role. To avoid undesired traffic loss, you can disable reversion to the original DF by enabling non-revertive mode for preference-based DF election.

Non-revertive mode for preference-based DF election takes effect after the **evpn df-election algorithm preference** command is executed in interface or system view.

Examples

Enable non-revertive mode for preference-based DF election.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn df-election preference non-revertive
```

Related commands

evpn df-election algorithm (interface view)

evpn df-election algorithm (system view)

evpn frr local (EVPN instance view/VSI EVPN instance view)

Use **evpn frr local enable** to enable local FRR on an EVPN instance.

Use **evpn frr local disable** to disable local FRR on an EVPN instance.

Use **undo evpn frr local** to restore the default.

Syntax

evpn frr local { disable | enable }

undo evpn frr local

Default

An EVPN instance uses the global local FRR configuration of EVPN VPLS.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Usage guidelines

Local FRR enables two PEs at a multihomed EVPN VPLS network site to set up a PW between them. This feature helps reduce the traffic loss caused by AC failure.

At a multihomed EVPN VPLS network site, CE 1 is dualhomed to PE 1 and PE 2, and PE 1 is the DF. When the AC on PE 1 fails, PE 1 deletes the corresponding MAC address entries and advertises the local unreachable event to PE 2 and remote PEs. Then, the remote PEs will switch traffic to the tunnels to PE 2. In this situation, PE 1 drops the packets that the remote PEs send before they are notified of the local unreachable event as the AC's MAC address entries have been deleted. To resolve this issue, enable local FRR on PE 1. If an AC fails, PE 1 changes the outgoing interface of the AC's MAC address entries to the index of the PW between PE 1 and PE 2. When receiving packets from remote PEs after its AC fails, PE 1 forwards the packets to PE 2 over the PW to prevent traffic loss.

On an EVPN instance, EVPN instance-specific local FRR configuration takes precedence over global local FRR configuration.

Examples

```
# Enable local FRR on the EVPN instance of VSI vpna.
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] evpn encapsulation mpls
[Sysname-vsi-vpna-evpn-mpls] evpn frr local enable
```

Related commands

evpn multihoming vpls-frr local

evpn multihoming advertise disable

Use **evpn multihoming advertise disable** to disable advertisement of EVPN multihoming routes and withdraw the EVPN multihoming routes that have been advertised to remote sites.

Use **undo evpn multihoming advertise disable** to restore the default.

Syntax

evpn multihoming advertise disable

undo evpn multihoming advertise disable

Default

The device advertises EVPN multihoming routes.

Views

System view

Predefined user roles

network-admin

Usage guidelines

EVPN multihoming routes include Ethernet auto-discovery routes and Ethernet segment routes.

In a multihomed EVPN network, execute this command on a redundant VTEP or PE before you reboot it. This operation allows other VTEPs or PEs to refresh their EVPN routing table to prevent traffic interruption caused by the reboot.

Examples

```
# Disable advertisement of EVPN multihoming routes and withdraw the EVPN multihoming routes that have been advertised to remote sites.
```

```
<Sysname> system-view
[Sysname] evpn multihoming advertise disable
```

evpn multihoming advertise ignore-ethernet-tag

Use **evpn multihoming advertise ignore-ethernet-tag** to enable the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes.

Use **undo evpn multihoming advertise ignore-ethernet-tag** to restore the default.

Syntax

evpn multihoming advertise ignore-ethernet-tag

undo evpn multihoming advertise ignore-ethernet-tag

Default

By default, the device advertises Ethernet auto-discovery routes and MAC/IP advertisement routes that carry Ethernet tags.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command on the redundant PEs or VTEPs at a dualhomed site.

This command enables the device to do the following:

- Withdraw the Ethernet auto-discovery routes and MAC/IP advertisement routes that have been advertised.
- Set the Ethernet tag to 0 for the Ethernet auto-discovery routes and MAC/IP advertisement routes and re-advertise them.

After you configure ESIs for ACs on the redundant edge devices at a dualhomed site, the edge devices advertise Ethernet auto-discovery routes and MAC/IP advertisement routes that carry Ethernet tags. If the remote peers are unable to identify Ethernet tags, you must execute this command on the redundant edge devices to enable communication with the peers.

When you use this command, follow these restrictions and guidelines:

- After you assign an ESI to a Layer 3 main interface, its subinterfaces inherit the ESI if they do not have one. In addition, you must map two subinterfaces to different VSIs if the subinterfaces have the same ESI.

Examples

```
# Enable the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes.
```

```
<Sysname> system-view
```

```
[Sysname] evpn multihoming advertise ignore-ethernet-tag
```

Related commands

esi

evpn multihoming vpls-frr local

Use **evpn multihoming vpls-frr local** to enable local FRR globally for EVPN VPLS.

Use **undo evpn multihoming vpls-frr local** to disable local FRR globally for EVPN VPLS.

Syntax

evpn multihoming vpls-frr local

undo evpn multihoming vpls-frr local

Default

Local FRR is disabled globally for EVPN VPLS.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Local FRR enables two PEs at a multihomed EVPN VPLS network site to set up a PW between them. This feature helps reduce the traffic loss caused by AC failure.

At a multihomed EVPN VPLS network site, CE 1 is dualhomed to PE 1 and PE 2, and PE 1 is the DF. When the AC on PE 1 fails, PE 1 deletes the corresponding MAC address entries and advertises the local unreachable event to PE 2 and remote PEs. Then, the remote PEs will switch traffic to the tunnels to PE 2. In this situation, PE 1 drops the packets that the remote PEs send before they are notified of the local unreachable event as the AC's MAC address entries have been deleted. To resolve this issue, enable local FRR on PE 1. If an AC fails, PE 1 changes the outgoing interface of the AC's MAC address entries to the index of the PW between PE 1 and PE 2. When receiving packets from remote PEs after its AC fails, PE 1 forwards the packets to PE 2 over the PW to prevent traffic loss.

On an EVPN instance, EVPN instance-specific local FRR configuration takes precedence over global local FRR configuration.

If you have executed the **evpn frr local** command on an EVPN instance, the **undo evpn multihoming vpls-frr local** command does not disable local FRR on the EVPN instance.

Examples

```
# Enable local FRR globally for EVPN VPLS.
<Sysname> system-view
[Sysname] evpn multihoming vpls-frr local
```

Related commands

evpn frr local (VSI EVPN instance view)

evpn multihoming re-originated mac

Use **evpn multihoming re-originated mac** to enable the device to generate MAC address entries for received MAC/IP advertisement routes.

Use **undo evpn multihoming re-originated mac** to restore the default.

Syntax

```
evpn multihoming re-originated mac
undo evpn multihoming re-originated mac
```

Default

The device does not generate MAC address entries for received MAC/IP advertisement routes.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command helps reduce the traffic loss caused by AC failure at a dualhomed EVPN VPLS network site.

At a multihomed EVPN VPLS network site, CE 1 is dualhomed to PE 1 and PE 2 through an aggregate link or smart trunk, and PE 3 is at a remote site. PE 1 forwards all traffic sent from CE 1 to the remote site, and PE 3 forwards the traffic that the remote site sends to CE 1 to both PE 1 and PE 2. When the AC on PE 1 fails, PE 1 withdraws the MAC/IP advertisement routes advertised to PE 2 and PE 3. In this situation, PE 3 does not have MAC address entries for CE 1 until PE 2 learns MAC address entries for CE 1 and advertises them to PE 3. As a result, traffic interruption occurs.

To resolve this issue, execute the **evpn multihoming re-originated mac** command on PE 2. When receiving the MAC/IP advertisement routes advertised by PE 1, PE 2 generates MAC address entries for the routes and advertises the entries to PE 3. PE 3 can use those MAC address entries to forward traffic to CE 1 when the AC on PE 1 fails.

You must enable local FRR for EVPN VPLS before you execute this command.

Examples

Enable the device to generate MAC address entries for received MAC/IP advertisement routes.

```
<Sysname> system-view
[Sysname] evpn multihoming re-originated mac
```

Related commands

evpn frr local (VSI EVPN instance view)

evpn multihoming vpls-frr local

evpn multihoming timer df-delay

Use **evpn multihoming timer df-delay** to set the DF election delay.

Use **undo evpn multihoming timer df-delay** to restore the default.

Syntax

evpn multihoming timer df-delay *delay-value*

undo evpn multihoming timer df-delay

Default

The DF election delay is 3 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

delay-value: Specifies the DF election delay, in the range of 1 to 1200 seconds.

Usage guidelines

DF election delay defines the minimum interval allowed between two DF elections.

The DF election can be triggered by site-facing interface status changes, redundant VTEP or PE membership changes, and interface ESI changes. To prevent frequent DF elections from degrading network performance, set the DF election delay.

To fast elect a DF and avoid traffic interruption upon DF failure, set the DF election delay to 0 seconds.

Examples

Set the DF election delay to 5 seconds.

```
<Sysname> system-view
[Sysname] evpn multihoming timer df-delay 5
```

evpn timer ad-delay

Use **evpn timer ad-delay** to set the advertisement delay timer for Ethernet auto-discovery routes.

Use **undo evpn timer ad-delay** to delete the advertisement delay setting for Ethernet auto-discovery routes.

Syntax

evpn timer ad-delay *delay-time*

undo evpn timer ad-delay

Default

Advertisement of Ethernet auto-discovery routes is not delayed.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay-time: Specifies a delay value in the range of 3 to 1200 seconds.

Usage guidelines

The advertisement delay timer for Ethernet auto-discovery routes helps reduce the traffic loss caused by a PE reboot at a multihomed EVPN VPLS network site.

At a multihomed EVPN VPLS network site, CE 1 is dualhomed to PE 1 and PE 2 through an aggregate link or smart trunk, and PE 3 is at a remote site. PE 1 forwards all traffic sent from CE 1 to the remote site, and PE 3 forwards the traffic that the remote site sends to CE 1 to both PE 1 and PE 2. When PE 1 reboots, it advertises Ethernet auto-discovery routes that carry next hop information to PE 3. If PE 3 has not received the MAC/IP advertisement routes advertised by PE 2 when receiving the Ethernet auto-discovery routes, it will forward traffic to both PE 1 and PE 2. In this situation, PE 1 does not have MAC address entries for CE 1 and drops the traffic.

To resolve this issue, set the advertisement delay timer for Ethernet auto-discovery routes on the CE-facing interface of PE 1. This timer allows PE 3 to receive the MAC/IP advertisement routes advertised by PE 2 before the Ethernet auto-discovery routes advertised by PE 1 and update its MAC address table timely.

Examples

On GigabitEthernet 1/0/1, set the advertisement delay timer for Ethernet auto-discovery routes to 300 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn timer ad-delay 300
```

evpn timer es-delay

Use **evpn timer es-delay** to set the advertisement delay timer for Ethernet segment routes.

Use **undo evpn timer es-delay** to delete the advertisement delay setting for Ethernet segment routes.

Syntax

evpn timer es-delay *delay-time*

undo evpn timer es-delay

Default

Advertisement of Ethernet segment routes is not delayed.

Views

Interface view

Predefined user roles

network-admin

Parameters

delay-time: Specifies a delay value in the range of 3 to 1200 seconds.

Usage guidelines

Use this command in combination with the **evpn track peer** command.

This **evpn track peer** excludes unavailable edge devices from DF election at a multihomed site. After an edge device recovers from failure and brings up its CE-facing interface, it starts the advertisement delay timer for Ethernet segment routes and checks the status of the BGP peer specified in this command. If the BGP peer comes up before the timer expires, the edge device advertises Ethernet segment routes to the peer. If the BGP peer is still down when the timer expires, the edge device does not advertise Ethernet segment routes to the peer. The edge devices then perform DF election based on the Ethernet segment routes they have received.

Examples

On GigabitEthernet 1/0/1, set the advertisement delay timer for Ethernet segment routes to 300 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn timer es-delay 300
```

Related commands

evpn track peer

evpn track peer

Use **evpn track peer** to enable the device to monitor the BGP peer status of another local edge device.

Use **undo evpn track peer** to restore the default.

Syntax

evpn track peer *peer-address*

undo evpn track peer

Default

At a multihomed site, the device does not monitor the BGP peer status of the other edge devices.

Views

Interface view

Predefined user roles

network-admin

Parameters

peer-address: Specifies a VTEP or PE by its IPv4 address.

Usage guidelines

Use this command on the CE-facing interfaces of the edge devices multihomed to a site to prevent device reboots from causing inter-site forwarding failure.

This command excludes unavailable edge devices from DF election at a multihomed site. After an edge device recovers from failure and brings up its CE-facing interface, it starts the advertisement delay timer for Ethernet segment routes and checks the status of the BGP peer specified in this command. If the BGP peer comes up before the timer expires, the edge device advertises Ethernet segment routes to the peer. If the BGP peer is still down when the timer expires, the edge device does not advertise Ethernet segment routes to the peer. The edge devices then perform DF election based on the Ethernet segment routes they have received.

Examples

On GigabitEthernet 1/0/1, enable the device to monitor the BGP peer at 1.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn track peer 1.1.1.1
```

Related commands

evpn timer es-delay

ignore-ac-state

Use **ignore-ac-state enable** to enable a VSI to ignore the state of ACs.

Use **ignore-ac-state disable** to disable a VSI from ignoring the state of ACs.

Use **undo ignore-ac-state** to restore the default.

Syntax

ignore-ac-state { enable | disable }

undo ignore-ac-state

Default

A VSI uses the global AC state ignore configuration.

Views

VSI view

Predefined user roles

network-admin

Usage guidelines

This command helps reduce the traffic loss caused by AC failure at a multihomed EVPN VPLS network site that uses single-active redundancy mode.

At a multihomed EVPN VPLS network site that uses single-active redundancy mode, CE 1 is dualhomed to PE 1 and PE 2 through a smart trunk. PE 1 is the primary PE, and PE 2 is the secondary PE. When the AC on PE 1 fails, PE 1 and PE 2 act as follows:

- PE 1 withdraws advertised Ethernet auto-discovery routes.
- PE 2 brings up its AC and advertises Ethernet auto-discovery routes to remote PEs.

The remote PEs switch traffic to the paths to PE 2 only after receiving the Ethernet auto-discovery routes advertised by PE 2, and traffic loss occurs during path switchover. To resolve this issue, enable VSIs to ignore the state of ACs on PE 2. This feature allows PE 2 to advertise Ethernet auto-discovery routes to remote PEs regardless of the state of ACs and speeds up path switchover when the AC on PE 1 fails.

On a VSI, VSI-specific AC state ignore configuration takes precedence over global AC state ignore configuration.

Use the **ignore-ac-state enable** command together with the **evpn multihoming re-originated mac** command.

Examples

```
# Enable VSI vpnna to ignore the state of ACs.
<Sysname> system-view
[Sysname] vsi vpnna
[Sysname-vsi-vpnna] ignore-ac-state enable
```

Related commands

l2vpn ignore-ac-state

l2vpn ignore-ac-state

Use **l2vpn ignore-ac-state** to enable VSIs to ignore the state of ACs globally.

Use **undo l2vpn ignore-ac-state** to disable VSIs from ignoring the state of ACs globally.

Syntax

l2vpn ignore-ac-state
undo l2vpn ignore-ac-state

Default

VSIs does not ignore the state of ACs.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command helps reduce the traffic loss caused by AC failure at a multihomed EVPN VPLS network site that uses single-active redundancy mode.

At a multihomed EVPN VPLS network site that uses single-active redundancy mode, CE 1 is dualhomed to PE 1 and PE 2 through a smart trunk. PE 1 is the primary PE, and PE 2 is the secondary PE. When the AC on PE 1 fails, PE 1 and PE 2 act as follows:

- PE 1 withdraws advertised Ethernet auto-discovery routes.
- PE 2 brings up its AC and advertises Ethernet auto-discovery routes to remote PEs.

The remote PEs switch traffic to the paths to PE 2 only after receiving the Ethernet auto-discovery routes advertised by PE 2, and traffic loss occurs during path switchover. To resolve this issue, enable VSIs to ignore the state of ACs on PE 2. This feature allows PE 2 to advertise Ethernet auto-discovery routes to remote PEs regardless of the state of ACs and speeds up path switchover when the AC on PE 1 fails.

On a VSI, VSI-specific AC state ignore configuration takes precedence over global AC state ignore configuration.

Use the **l2vpn ignore-ac-state** command together with the **evpn multihoming re-originated mac** command.

Examples

```
# Enable VSIs to ignore the state of ACs globally.
<Sysname> system-view
[Sysname] l2vpn ignore-ac-state
```

Related commands

ignore-ac-state

pw-class

Use **pw-class** to specify a PW class for a VSI EVPN instance.

Use **undo pw-class** to restore the default.

Syntax

pw-class *class-name*

undo pw-class

Default

No PW class is specified for a VSI EVPN instance.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Parameters

class-name: Specifies a PW class by its name, a case-sensitive string of 1 to 19 characters.

Usage guidelines

This command is supported only by EVPN instances that use MPLS encapsulation.

The specified PW class will be used to establish all PWs on the VSI EVPN instance.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify PW class **pw100** for the EVPN instance on VSI **vpna**.

```
<Sysname> system-view
[Sysname] vsi vpna
[Sysname-vsi-vpna] evpn encapsulation mpls
[Sysname-vsi-vpna-evpn-mpls] pw-class pw100
```

tunnel-policy

Use **tunnel-policy** to specify a tunnel policy for a VSI EVPN instance.

Use **undo tunnel-policy** to restore the default.

Syntax

tunnel-policy *tunnel-policy-name*

undo tunnel-policy

Default

No tunnel policy is specified for a VSI EVPN instance.

Views

VSI EVPN instance view

Predefined user roles

network-admin

Parameters

tunnel-policy-name: Specifies a tunnel policy by its name, a case-sensitive string of 1 to 19 characters.

Usage guidelines

This command is supported only by EVPN instances that use MPLS encapsulation.

The PWs of the VSI EVPN instance use the specified tunnel policy to select public tunnels.

If you do not specify a tunnel policy or specify a nonexistent tunnel policy, the default tunnel policy applies. The default tunnel policy selects only one public tunnel for a PW in this order: LSP tunnel, GRE tunnel, CRLSP tunnel, and SRLSP tunnel.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify tunnel policy **policy1** for the EVPN instance on VSI **aa**.

```
<Sysname> system-view
[Sysname] vsi aa
[Sysname-vsi-aa] evpn encapsulation mpls
[Sysname-vsi-aa-evpn-mpls] tunnel-policy policy1
```

Modified command: display evpn auto-discovery

Old syntax

```
display evpn auto-discovery { imet [ peer ip-address ] [ vsi vsi-name ] | macip-prefix
[ nexthop next-hop ] [ count ] }
```

New syntax

```
display evpn auto-discovery { { imet | mac-ip } [ mpls | srv6 | vxlan ] [ peer
ip-address ] [ vsi vsi-name ] | macip-prefix [ nexthop next-hop ] [ count ] }
```

Views

Any view

Change description

The following keywords were added:

mac-ip: Specifies MAC/IP advertisement routes.

mpls: Specifies the EVPN VPLS network.

srv6: Specifies the EVPN VPLS over SRv6 network.

vxlan: Specifies the EVPN VXLAN network.

Modified command: display evpn route mac

Old syntax

```
display evpn route mac [ local | remote ] [ vsi vsi-name ] [ count ]
```

New syntax

```
display evpn route mac [ mpls | srv6 | vxlan ] [ local | remote ] [ vsi vsi-name ]  
[ count ]
```

Views

Any view

Change description

The following keywords were added:

mpls: Specifies the EVPN VPLS network.

srv6: Specifies the EVPN VPLS over SRv6 network. For more information about EVPN VPLS over SRv6, see *Segment Routing Configuration Guide*.

vxlan: Specifies the EVPN VXLAN network.

Modified command: evpn encapsulation

Old syntax

In VSI view:

```
evpn encapsulation vxlan
```

```
undo evpn encapsulation
```

New syntax

In VSI view:

```
evpn encapsulation { mpls | vxlan }
```

```
undo evpn encapsulation
```

In cross-connect group view:

```
evpn encapsulation mpls
```

```
undo evpn encapsulation
```

Views

VSI view

Cross-connect group view

Change description

The following keyword was added:

mpls: Specifies MPLS encapsulation.

This command was added in cross-connect group view

New feature: EVPN VPWS

About EVPN VPWS

EVPN Virtual Private Wire Service (VPWS) is a Layer 2 VPN technology that uses MP-BGP for BGP EVPN route advertisement in the control plane and MPLS for forwarding in the data plane. EVPN VPWS provides point-to-point forwarding services for users by using ACs and PWs associated with cross-connects without MAC address table lookup.

EVPN VPWS network model

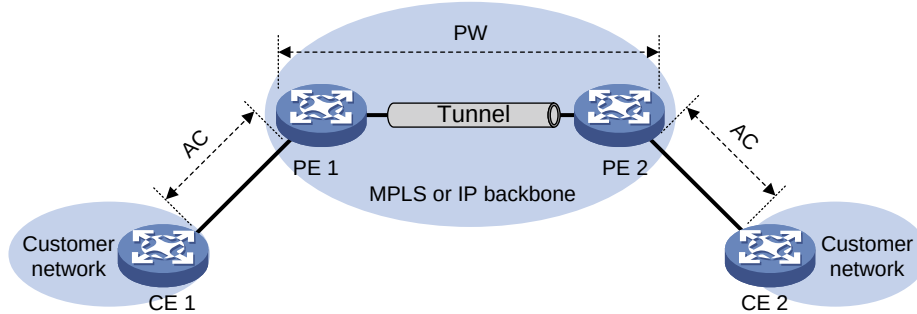
As shown in [Figure 46](#), an EVPN VPWS network contains the following devices:

- **Customer edge (CE)**—Customer device directly connected to the service provider network.
- **Provider edge (PE)**—Service provider device connected to CEs. PEs provide access to the EVPN VPWS network and forward traffic between customer network sites by using public tunnels.

A PE uses ACs, PWs, tunnels, and cross-connects to provide EVPN VPWS services.

- **Attachment circuit (AC)**—A physical or virtual link between a CE and a PE.
- **Pseudowire (PW)**—A virtual bidirectional connection between two PEs. A PW comprises a pair of virtual connections in opposite directions.
- **Public tunnel**—A connection that carries one or more PWs across the MPLS or IP backbone. A public tunnel can be an LSP, GRE tunnel, or MPLS TE tunnel.
- **Cross-connect**—A connection formed by two physical or virtual circuits such as ACs and PWs. It switches packets between the two physical or virtual circuits. Cross-connects include AC to AC cross-connect and AC to PW cross-connect.

Figure 54 EVPN VPWS network



Remote connection establishment

EVPN VPWS remote connection provides point-to-point Layer 2 connectivity between customer network sites by using PWs over an IP or MPLS backbone.

To set up a remote EVPN VPWS connection:

1. Set up a public tunnel to carry one or more PWs between PEs.
2. Set up a PW to connect customer networks.
3. Set up an AC between a PE and a CE.
4. Bind the AC to the PW.

After the PE receives packets from the AC, it adds the PW label into the packets and sends the packets to the peer PE through the public tunnel.

After the peer PE receives the packets from the public tunnel, it removes the PW label of the packets and forwards the packets to the AC bound to the PW.

Public tunnel establishment

The public tunnel can be an LSP, MPLS TE, or GRE tunnel.

If multiple public tunnels are set up between two PEs, you can configure a tunnel policy to control tunnel selection. For more information about tunnel policies, see *MPLS Configuration Guide*.

If a PW is established over an LSP or MPLS TE tunnel, packets on the PW have two labels. The outer label is the public LSP or MPLS TE tunnel label that MPLS uses to forward the packet to the

peer PE. The inner label is the PW label that the peer PE uses to forward the packet to the destination CE.

PW establishment

A PW is established between two PEs based on the local and remote service IDs configured on the PEs. In an EVPN VPWS network, each PE advertises its local service ID through Ethernet auto-discovery routes and compares received local service IDs with its remote service ID. A PE establishes a unidirectional virtual connection to a peer PE if the local service ID advertised by the peer matches the remote service ID. PW establishment is finished when two virtual connections in opposite directions are established between two PEs.

AC establishment

For EVPN VPWS, an AC is associated with a cross-connect and can be a Layer 3 Ethernet interface or Layer 3 Ethernet subinterface.

AC-to-PW bindings

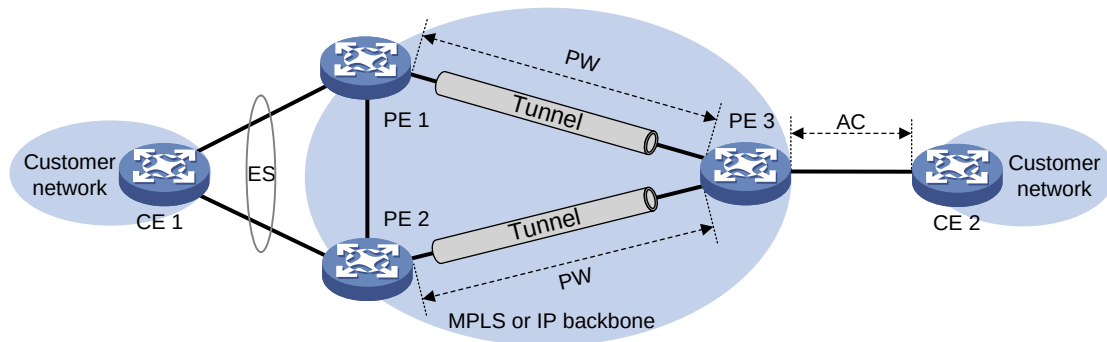
For PEs to forward packets between an AC and a PW, bind the AC to the PW.

EVPN VPWS multihoming

About this task

As shown in [Figure 47](#), EVPN VPWS supports deploying multiple PEs at a site for redundancy and high availability. On the redundant PEs, Ethernet links connected to the site form an ES that is uniquely identified by an ESI. EVPN VPWS supports only dualhoming.

Figure 55 EVPN VPWS multihoming

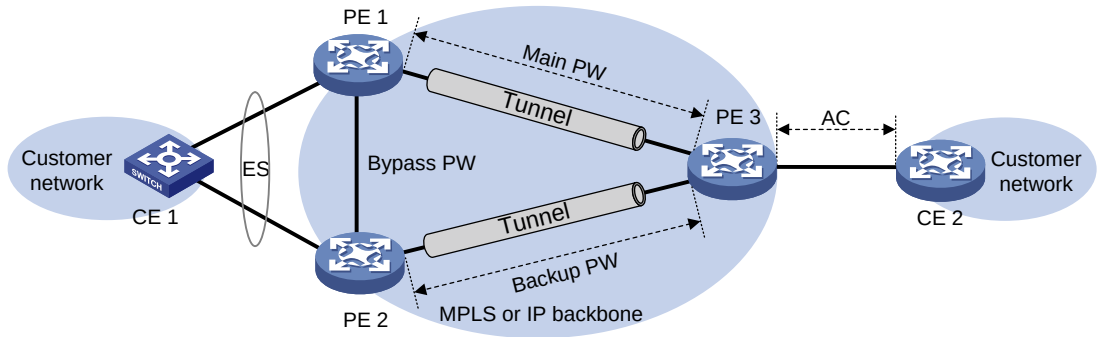


Redundancy mode

The device supports single-active redundancy mode and all-active redundancy mode of EVPN VPWS multihoming.

- **Single-active mode**—This mode allows one of the redundant PWs to forward traffic, as shown in [Figure 56](#). When the main PW becomes unavailable because of device failure or link failure, traffic is switched to the backup PW for forwarding. The redundant PEs elect the main PW as described in "[DF election](#)". To ensure quick failover, EAA CLI-defined monitor policies and Track are configured on the CE-facing physical interface and the transport-facing physical interface used for establishing the main PW on PE 1. When the underlay network is disconnected, PE 1 shuts down the CE-facing physical interface so all traffic of CE 1 is forwarded through PE 2. For more information about EAA, see *Network Management and Monitoring Configuration Guide*.

Figure 56 Single-active mode



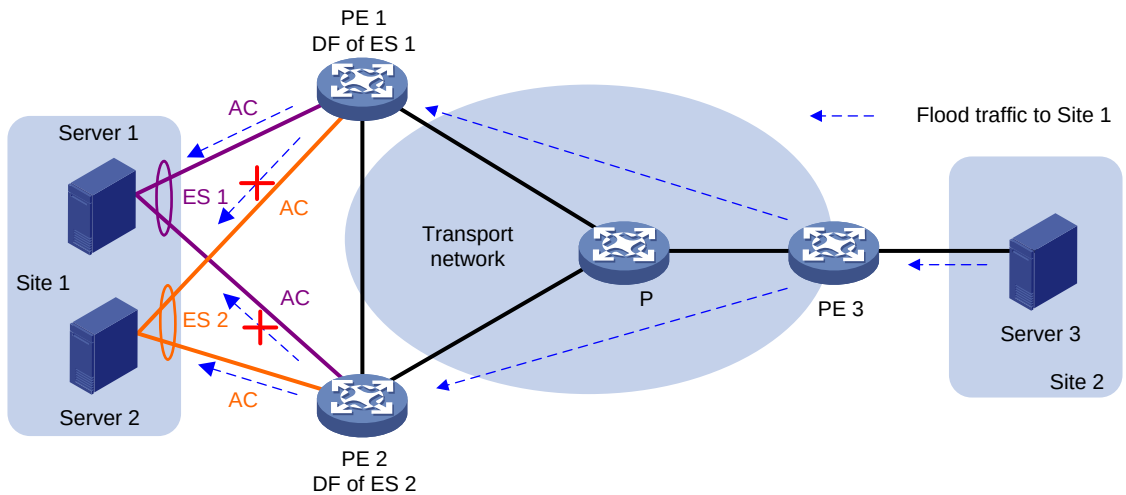
- **All-active mode**—This mode allows all redundant PWs to a multihomed site to load share traffic. To ensure quick failover, EAA CLI-defined monitor policies and Track are configured on the CE-facing physical interface and the transport-facing physical interface used for establishing a PW on each redundant PE.

About DF election

In single-active mode, a DF is elected from the redundant PEs to determine the main PW. PEs that fail the election are assigned the BDF role. The PWs on BDFs do not forward traffic.

Redundant PEs at a site send Ethernet segment routes to one another to advertise ES and PE IP mappings. A PE accepts the Ethernet segment routes only when it is configured with an ESI. Then, the PEs select a DF based on the ES and PE IP mappings. DF election can be performed by using a VLAN tag-based algorithm or preference-based algorithm.

Figure 57 DF election



VLAN tag-based DF election

PEs select a DF for each AC based on the VLAN tag and PE IP address as follows:

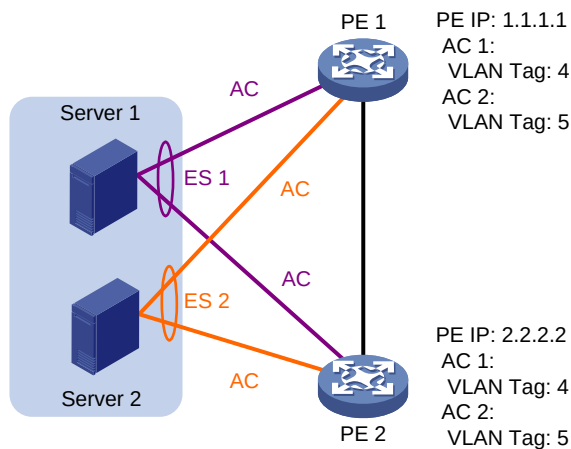
1. Arrange source IP addresses in Ethernet segment routes with the same ESI in ascending order and assign a sequence number to each IP address, starting from 0.
2. Divide the lowest VLAN ID permitted on an AC by the number of the redundant PEs, and match the remainder to the sequence numbers of IP addresses.
3. Assign the DF role to the PE that uses the IP address with the matching sequence number.

The following uses PE 1 and PE 2 in Figure 49 as an example to explain the DF election procedure:

4. PE 1 and PE 2 send Ethernet segment routes to each other.

5. The PEs assign sequence numbers 0 and 1 to IP addresses 1.1.1.1 and 2.2.2.2 in the Ethernet segment routes, respectively.
6. The PEs divide 4 (the lowest VLAN ID permitted by the ACs) by 2 (the number of redundant PEs), and match the remainder 0 to the sequence numbers of the IP addresses.
7. The DF role is assigned to PE 1 at 1.1.1.1.

Figure 58 VLAN tag-based DF election



Preference-based DF election

PEs select a DF for each ES based on the DF election preference, the Don't Preempt Me (DP) bit in Ethernet segment routes, and PE IP address. The DP bit can be set to one of the following values:

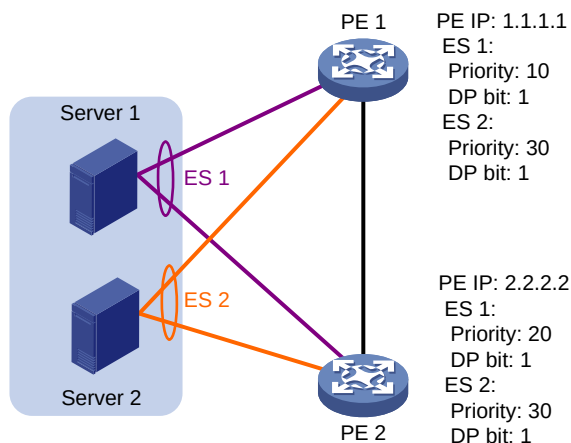
- **1**—DF preemption is disabled. A DF retains its role when a new DF is elected.
- **0**—DF preemption is enabled.

Preference-based DF election uses the following rules to select a DF for an ES:

- The PE with higher preference becomes the DF.
- If two PEs have the same preference, the PE with the DP bit set to 1 becomes the DF. If both of the PEs have the DP bit set to 1, the PE with a lower IP address becomes the DF.

As shown in [Figure 50](#), PE 2 is the DF for ES 1, and PE 1 is the DF for ES 2.

Figure 59 Preference-based DF election



FRR for EVPN VPWS

About FRR

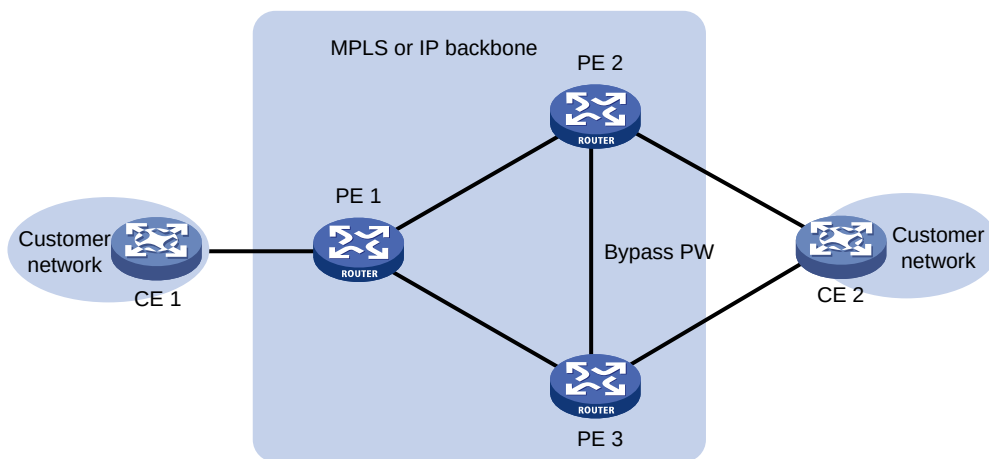
Fast reroute (FRR) helps reduce the traffic loss caused by AC or PW failure on an EVPN VPWS network. FRR includes local FRR and remote FRR.

Local FRR

Local FRR enables two PEs at a multihomed EVPN VPWS network site to set up a bypass PW between them.

As shown in [Figure 51](#), CE 2 is dualhomed to PE 2 and PE 3. When the AC on PE 2 fails, PE 2 advertises the local unreachable event to PE 1 and PE 3 for PE 1 to switch traffic to the PW to PE 3. In this situation, PE 3 drops the packets that PE 1 sends before it is notified of the local unreachable event. To resolve this issue, enable local FRR on PE 2 and PE 3. When receiving packets from PE 1 after PE 2's AC fails, PE 2 forwards the packets to PE 3 over the bypass PW to prevent traffic loss.

Figure 60 Local FRR

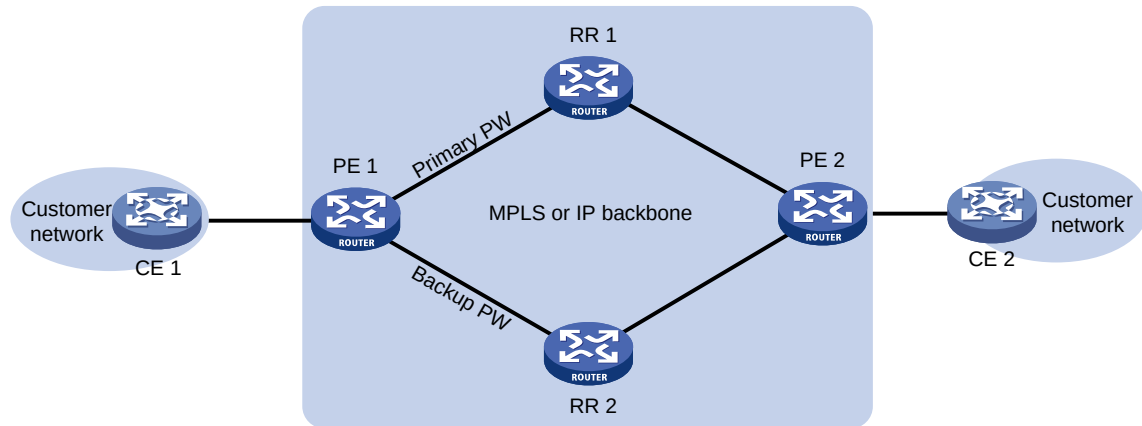


Remote FRR

Remote FRR enables two PEs on an EVPN VPWS network to set up a primary PW and a backup PW between them to ensure high availability. This feature is applicable to both multihoming and singlehoming scenarios.

As shown in [Figure 61](#), PE 1 and PE 2 are connected by RR 1 and RR 2. The RRs change the next hop attribute of routes and reassign MPLS labels to them based on routing policies when reflecting the routes. PE 1 and PE 2 select only RR 1 or RR 2 when establishing a PW. For high availability, you can enable remote FRR on PE 1 for it to set up PWs to both RRs. PE 1 uses the primary PW to forward traffic as long as it is available. When the primary PW fails, PE 1 switches traffic to the backup PW. For more information about optimal route selection on PE 1, see BGP configuration in *Layer 3—IP Routing Configuration Guide*.

Figure 61 Remote FRR



Control word

The control word field is between the MPLS label stack and the Layer 2 data. It carries control information for the Layer 2 frame, for example, the sequence number.

The control word feature has the following functions:

- Avoids fragment disorder. In multipath forwarding, fragments received might be disordered. The control word feature reorders the fragments according to the sequence number carried in the control word field.
- Identifies the original payload length for packets that include padding.

The control word field is optional for EVPN PWs. You can configure whether to carry the control word field in packets sent on the PW. If you enable the control word feature on both PEs, packets transmitted on the PW carry the control word field. Otherwise, the packets do not carry the control word field.

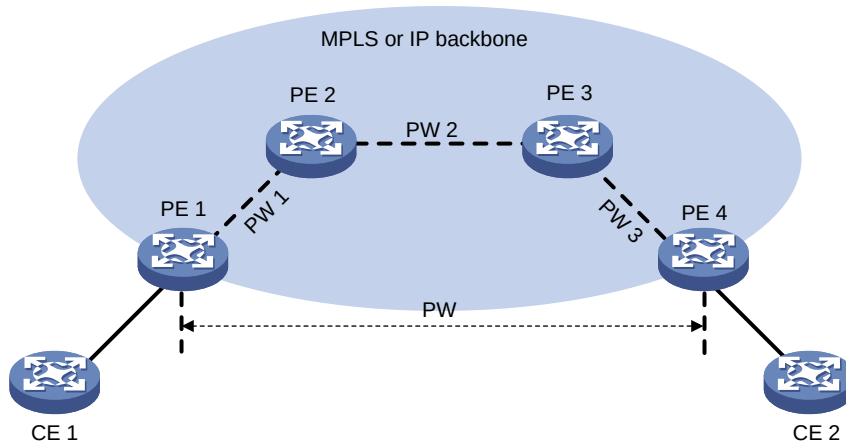
PW concatenation

As shown in [Figure 62](#), EVPN VPWS supports concatenating two or more PWs into one PW. PW concatenation allows two PEs that do not have an end-to-end public tunnel between them to communicate. An intermediate PE forwards packets between two concatenated PWs as follows:

1. Removes the tunnel identifier and PW label from the packets received on one PW.
2. Encapsulates the packets with the label of another PW and forwards them through the public tunnel that conveys this PW.

Two PWs are concatenated by creating them on the same cross-connect. For example, to concatenate PW 1 and PW 2 in [Figure 62](#), create them on the same cross-connect on PE 2.

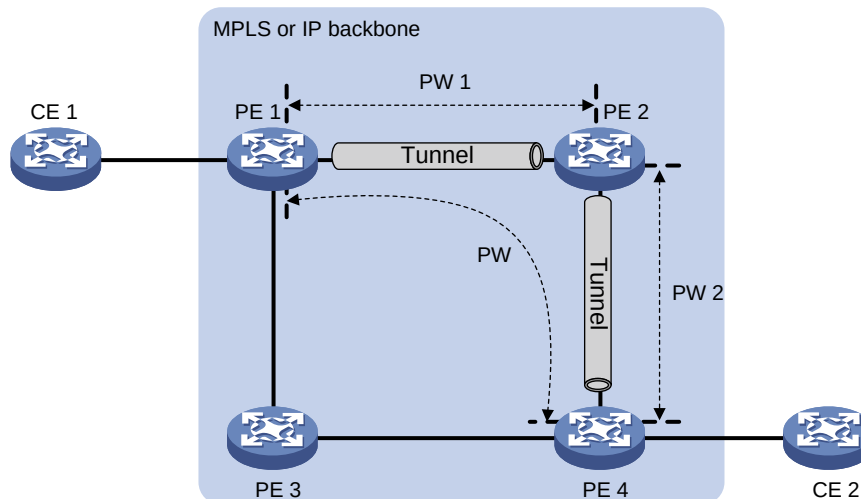
Figure 62 PW concatenation



PW concatenation includes intra-AS PW concatenation and inter-AS PW concatenation.

- **Intra-AS PW concatenation**—Concatenates PWs within an AS. As shown in [Figure 63](#), all PEs are in the same AS, and no end-to-end public tunnel exists between PE 1 and PE 4. By concatenating PW 1 and PW 2, you can enable PE 1 and PE 4 to communicate through the existing public tunnels instead of creating a new one.

Figure 63 Intra-AS PW concatenation



- **Inter-AS PW concatenation**—Concatenates PWs in different ASs. For more information, see "Inter-AS option B."

Inter-AS communication of EVPN VPWS

In an inter-AS networking scenario, multiple sites of an EVPN VPWS network are connected to multiple ISPs in different ASs, or to multiple ASs of an ISP.

EVPN VPWS provides the following inter-AS communication solutions:

- **Inter-AS option A**—Associates the AC between ASBRs with each EVPN PW established between a PE and ASBR pair.
- **Inter-AS option B**—Establishes an EVPN PW between ASBRs and concatenates it with the EVPN PWs established between PE and ASBR pairs.

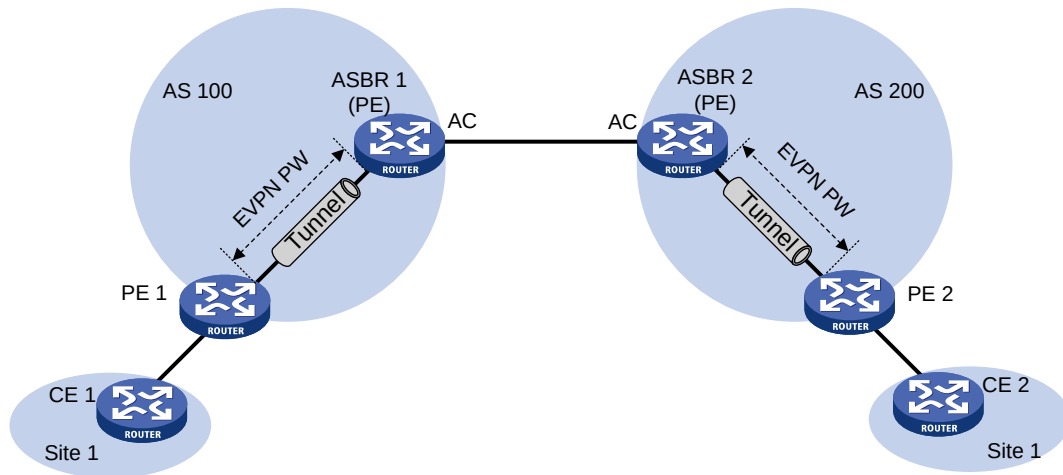
- **Inter-AS option C**—Establishes an EVPN PW between PEs in different ASs through a multihop MP-EBGP session.

Inter-AS option A

As shown in [Figure 64](#), in this solution, PEs of two ASs are directly connected, and each PE is also the ASBR of its AS. Each PE treats the other as a CE and associates its EVPN PW with the interface facing the peer PE for inter-AS communication.

This solution features simple implementation. You need to configure only EVPN PW and AC associations for each site on the PEs that act as ASBRs. However, the management workload increases if more sites are attached to the ASBRs.

Figure 64 Inter-AS option A network model

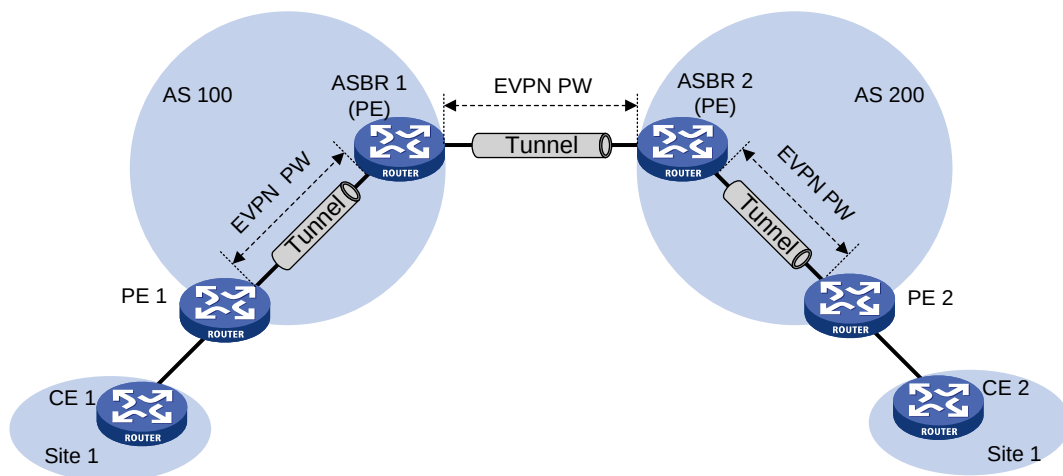


Inter-AS option B

As shown in [Figure 65](#), in this solution, an EVPN PW is established between the ASBRs for inter-AS communication. The ASBRs use MP-EBGP to exchange BGP EVPN routes to establish the EVPN PW. The PE and the ASBR in each AS use MP-IBGP to establish an EVPN PW. The EVPN PWs between the ASBRs and between each PE and ASBR pair are concatenated to forward inter-AS traffic.

This solution provides better scalability than inter-AS option A. To use this solution, you need to configure PW concatenation for each pair of sites.

Figure 65 Inter-AS option B network model



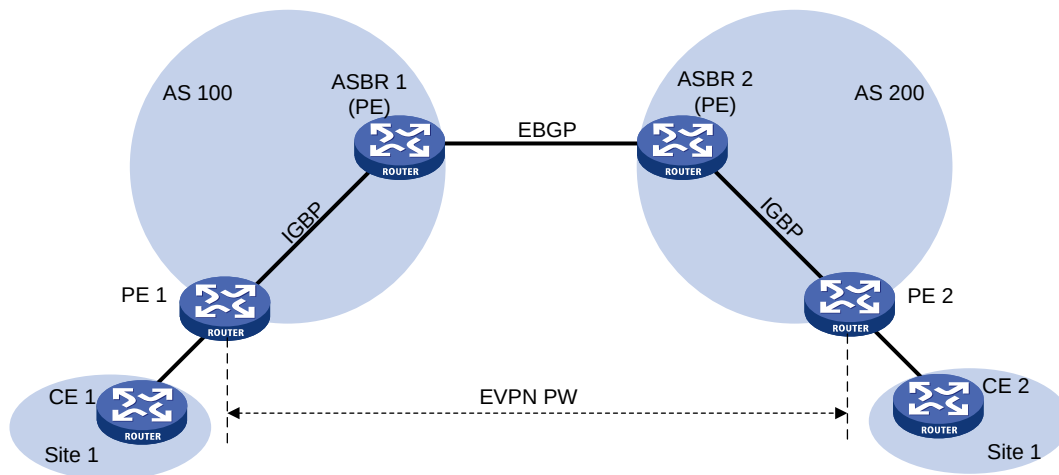
Inter-AS option C

As shown in Figure 66, in this solution, PEs in different ASs establish a multihop MP-EBGP session to exchange BGP EVPN routes and create an EVPN PW. Each PE must have a route to the peer PE and a label for the route so that the inter-AS public tunnel can be set up between the PEs. Inter-AS option C sets up a public tunnel by using the following methods:

- A label distribution protocol within the AS, for example, LDP.
- Labeled IPv4 unicast route advertisement by ASBRs through BGP.

Labeled IPv4 unicast route advertisement refers to the process of assigning MPLS labels to IPv4 unicast routes and advertising IPv4 unicast routes and their labels.

Figure 66 Inter-AS option C network model



The following is the process for setting up a public tunnel between PE 1 and PE 2 in Figure 66:

2. Within AS 100, the public tunnel from ASBR 1 to PE 1 is set up by using a label distribution protocol, for example, LDP.
Assume that the outgoing label for the public tunnel on ASBR 1 is L1.
3. ASBR 1 advertises labeled IPv4 unicast routes to ASBR 2 through EBGP.
The route destined for PE 1 and the label (L2) assigned by ASBR 1 to the route are advertised from ASBR 1 to ASBR 2. The next hop of the route is ASBR 1. The public tunnel from ASBR 2 to ASBR 1 is set up. The incoming label for the public tunnel on ASBR 1 is L2.
4. ASBR 2 advertises labeled IPv4 unicast routes to PE 2 through IGBP.
The route destined for PE 1 and the label (L3) assigned by ASBR 2 to the route are advertised from ASBR 2 to PE 2. The next hop for the route is ASBR 2. The public tunnel from PE 2 to ASBR 2 is set up. The incoming label for the public tunnel on ASBR 2 is L3, and the outgoing label is L2.
5. MPLS packets cannot be forwarded directly from PE 2 to ASBR 2. Within AS 200, the public tunnel from PE 2 to ASBR 2 is required to be set up hop by hop through a label distribution protocol, for example, LDP.

Assume that the outgoing label for the public tunnel on PE 3 is Lv.

After route advertisement and public tunnel setup, PE 1 and PE 2 set up a multihop MP-EBGP session to establish an EVPN PW. You must associate the EVPN PW with an AC on PE 1 and PE 2 to enable inter-AS forwarding.

To improve scalability, you can specify a RR in each AS to exchange BGP EVPN routes with PEs in the same AS. The RR in each AS maintains all BGP EVPN routes. The RRs in two ASs establish a multihop MP-EBGP session to advertise BGP EVPN routes.

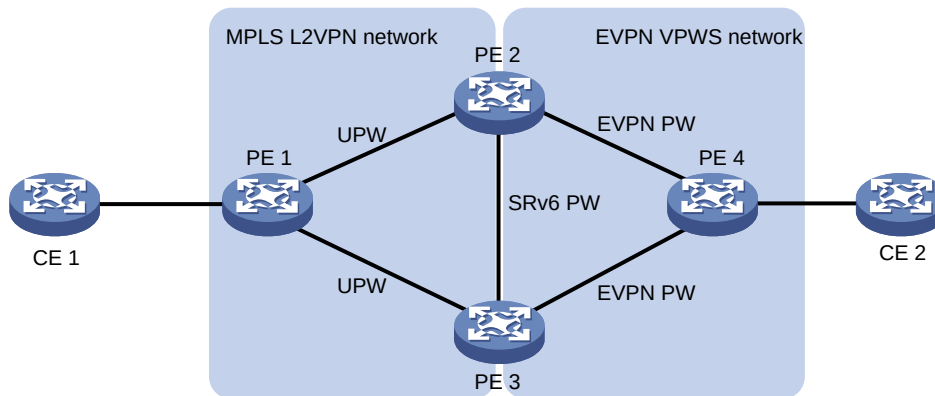
Inter-AS option C features the best scalability. It allows PEs to directly exchange BGP EVPN routes. The ASBRs do not maintain or advertise BGP EVPN routes.

LDP or static PW ACs for EVPN PWs

This feature ensures that a traditional MPLS L2VPN (VPWS) network and an EVPN VPWS network can communicate with each other. The LDP or static PWs in the VPWS network are configured as ACs to the EVPN VPWS network. These ACs are referred to as UPWs in the EVPN VPWS network. Packets are forwards between EVPN PWs and UPWs, so the VPWS and EVPN VPWS networks can communicate with each other.

With this feature, a PE in the VPWS network can be single-homed or dual-homed to an EVPN VPWS network. As shown in Figure 67, PE 1 in the VPWS network is connected to PE 2 and PE 3 through LDP or static PWs. One of the PWs is the primary PW and the other PW is the backup PW. The PWs are UPWs. In the EVPN VPWS network, PE 4 is connected to PE 2 and PE 3 through EVPN PWs. The UPWs in the VPWS network act as ACs to the EVPN VPWS network. When PE 2 or PE 3 receives packets from the UPWs, it removes MPLS encapsulation from the packets and looks up the MAC address table for a matching EVPN PW. Then, the PE adds MPLS encapsulation to the packets and forwards the packets through the matching EVPN PW to PE 4. When PE 2 or PE 3 receives packets from an EVPN PW, it uses the same procedure to process the packets.

Figure 67 LDP or static PW ACs for EVPN PWs



EVPN VPWS tasks at a glance

Configuring a remote connection

To configure a remote connection, perform the following tasks:

1. Enabling L2VPN
2. Configuring a Layer 3 interface with Ethernet or VLAN encapsulation
3. Configuring EVPN route advertisement
 - Enabling BGP to advertise BGP EVPN routes
 - Enabling the device to advertise MPLS-encapsulated BGP EVPN routes
 - (Optional.) Configuring optimal route selection and route advertisement settings
 - (Optional.) Maintaining BGP sessions
4. Configuring a cross-connect
5. Configuring a PW
 - a. (Optional.) Configuring a PW class
 - b. Configuring an EVPN PW
6. Mapping an AC to a cross-connect
7. (Optional.) Configuring EVPN VPWS multihoming

- a. Assigning an ESI to an interface
- b. (Optional.) Configuring the DF election algorithm
- c. (Optional.) Setting the redundancy mode on an interface
- d. (Optional.) Setting the DF election delay
- e. (Optional.) Disabling advertisement of EVPN multihoming routes
- f. (Optional.) Enabling the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes
- g. (Optional.) Enabling the device to monitor the BGP peer status of another local edge device
- 8. (Optional.) Configuring FRR for EVPN VPWS
 - o Configuring local FRR
 - o Configuring remote FRR
- 9. (Optional.) Configuring LDP or static PWs as ACs for EVPN PWs

Configuring PW concatenation

To configure PW concatenation, perform the following tasks:

1. Enabling L2VPN
2. Configuring a cross-connect
3. Configuring a PW

To concatenate two PWs, create them on the same cross-connect.

- a. (Optional.) Configuring a PW class
- b. Configuring an EVPN PW

Restrictions and guidelines: S-trunk support

The device does not support S-trunk.

Prerequisites for EVPN VPWS

To configure EVPN VPWS, you must perform the following tasks:

1. Configure an IGP to achieve IP connectivity within the backbone.
2. Configure basic MPLS, LDP, GRE, or MPLS TE to set up public tunnels across the backbone.

Enabling L2VPN

Prerequisites

Before you enable L2VPN, perform the following tasks:

- Configure an LSR ID for the PE by using the **mpls lsr-id** command.
- Enable MPLS by using the **mpls enable** command on the transport-facing interface of the PE.

For more information about the **mpls lsr-id** and **mpls enable** commands, see *MPLS Command Reference*.

Procedure

1. Enter system view.
system-view

2. Enable L2VPN.

l2vpn enable

By default, L2VPN is disabled.

Configuring a Layer 3 interface with Ethernet or VLAN encapsulation

About this task

Configure a Layer 3 interface on a PE to establish an AC to the CE. On a Layer 3 Ethernet interface (including Layer 3 Ethernet interface, Layer 3 virtual Ethernet interface, and VE-L2VPN interface), both the PW data encapsulation type and access mode are Ethernet. On a Layer 3 Ethernet subinterface, both the PW data encapsulation type and access mode are VLAN.

Restrictions and guidelines

The PE forwards packets received from a Layer 3 interface through the bound PW without network layer processing. Therefore, the Layer 3 interface does not need an IP address.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*

Configuring EVPN route advertisement

Restrictions and guidelines for EVPN route advertisement configuration

For more information about the BGP commands used in this task, see *Layer 3—IP Routing Command Reference*.

Enabling BGP to advertise BGP EVPN routes

1. Enter system view.
system-view
2. Configure a global router ID.
router id *router-id*
By default, no global router ID is configured.
3. Enable a BGP instance and enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
By default, BGP is disabled and no BGP instances exist.
4. Specify remote PEs as BGP peers.
peer { *group-name* | *ipv4-address* [*mask-length*] } **as-number** *as-number*
5. Create the BGP EVPN address family and enter BGP EVPN address family view.
address-family **l2vpn evpn**

6. Enable BGP to exchange BGP EVPN routes with a peer or peer group.

```
peer { group-name | ipv4-address [ mask-length ] } enable
```

By default, BGP does not exchange BGP EVPN routes with peers.

Enabling the device to advertise MPLS-encapsulated BGP EVPN routes

About this task

Perform this task on PEs for them to establish PWs.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP EVPN address family view.
address-family **l2vpn evpn**
4. Enable MPLS encapsulation for the BGP EVPN routes advertised to a peer or peer group.
peer { *group name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
advertise encaps-type mpls
By default, BGP EVPN routes use VXLAN encapsulation.

Configuring optimal route selection and route advertisement settings

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp *as-number* [**instance** *instance-name*]
3. Enter BGP EVPN address family view.
address-family **l2vpn evpn**
4. Permit the local AS number to appear in routes from a peer or peer group and set the number of appearances.
peer { *group-name* | *ipv4-address* [*mask-length*] } **allow-as-loop** [*number*]
By default, the local AS number is not allowed in routes from peers.
5. Enable route target filtering for BGP EVPN routes.
policy **vpn-target**
By default, route target filtering is enabled for BGP EVPN routes.
6. Prefer routes learned from the specified peer or peer group during optimal route selection.
peer { *group-name* | *ipv4-address* [*mask-length*] | *ipv6-address* [*prefix-length*] }
high-priority

By default, BGP does not prefer routes learned from any peer or peer groups during optimal route selection.

7. Configure BGP route reflection settings:

- a. Configure the device as an RR and specify a peer or peer group as its client.

peer { *group-name* | *ipv4-address* [*mask-length*] } **reflect-client**

By default, no RR or client is configured.

- b. (Optional.) Enable BGP EVPN route reflection between clients.

reflect between-clients

By default, BGP EVPN route reflection between clients is enabled.

- c. (Optional.) Configure the cluster ID of the RR.

reflector cluster-id { *cluster-id* | *ipv4-address* }

By default, an RR uses its own router ID as the cluster ID.

- d. (Optional.) Create a reflection policy for the RR to filter reflected BGP EVPN routes.

rr-filter { *ext-comm-list-number* | *ext-comm-list-name* }

By default, an RR does not filter reflected BGP EVPN routes.

- e. (Optional.) Create a reflection policy for the RR to filter reflected BGP EVPN routes.

reflect change-path-attribute

By default, an RR does not filter reflected BGP EVPN routes.

8. Configure the device to not change the next hop of routes advertised to an EBGp peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **next-hop-invariable**

By default, the device uses its address as the next hop of routes advertised to EBGp peers.

9. Apply a routing policy to routes received from or advertised to a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **route-policy** *route-policy-name*
{ **export** | **import** }

By default, no routing policies are applied to routes received from or advertised to peers or peer groups.

10. Advertise the COMMUNITY attribute to a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise-community**

By default, the device does not advertise the COMMUNITY attribute to peers or peer groups.

11. Configure the BGP Add-Path feature:

- o Configure the BGP additional path capabilities.

peer { *group-name* | *ipv4-address* [*mask-length*] } **additional-paths** { **receive** | **send** } *

By default, no BGP additional path capabilities are configured.

- o Set the maximum number of Add-Path optimal routes that can be advertised to a peer or peer group.

peer { *group-name* | *ipv4-address* [*mask-length*] } **advertise additional-paths**
best number

By default, a maximum number of one Add-Path optimal route can be advertised to a peer or peer group.

- o Set the maximum number of Add-Path optimal routes that can be advertised to all peers.

additional-paths select-best *best-number*

By default, a maximum number of one Add-Path optimal route can be advertised to all peers.

Maintaining BGP sessions

Perform the following tasks in user view:

- Reset BGP sessions of the BGP EVPN address family.

```
reset bgp [ instance instance-name ] { as-number | ipv4-address [ mask-length ] |  
ipv6-address [ prefix-length ] } | all | external | group group-name | internal } l2vpn  
evpn
```

- Soft-reset BGP sessions of the BGP EVPN address family.

```
refresh bgp [ instance instance-name ] { ipv4-address [ mask-length ] | ipv6-address  
[ prefix-length ] } | all | external | group group-name | internal } { export | import }  
l2vpn evpn
```

Configuring a cross-connect

Restrictions and guidelines

For more information about the cross-connect commands used in this task, see MPLS L2VPN commands in *MPLS Command Reference*.

Procedure

- Enter system view.
system-view
- Create a cross-connect group and enter cross-connect group view.
xconnect-group *group-name*
- (Optional.) Configure a description for the cross-connect group.
description *text*
By default, no description is configured for a cross-connect group.
- (Optional.) Enable the cross-connect group.
undo shutdown
By default, the cross-connect group is enabled.
- Create a cross-connect and enter cross-connect view.
connection *connection-name*

Configuring a PW

Configuring a PW class

About this task

You can configure PW attributes such as the PW data encapsulation type and enable control word in a PW class. PWs with the same attributes can use the same PW class.

Restrictions and guidelines

For more information about the PW class commands used in this task, see MPLS L2VPN commands in *MPLS Command Reference*.

You must configure the same data encapsulation type on two PEs that are connected by the same PW.

For correct PW setup, make sure the status of the control word feature is the same on the two PEs that are connected by the same PW.

Procedure

1. Enter system view.
system-view
2. Create a PW class and enter PW class view.
pw-class *class-name*
3. Enable control word.
control-word enable
By default, control word is disabled.
4. Specify the PW data encapsulation type.
pw-type { **ethernet** | **vlan** }
By default, the PW data encapsulation type is VLAN.

Configuring an EVPN PW

About this task

To establish an EVPN PW between two PEs, specify a local service ID and a remote service ID on both PEs. The local service ID specified on one PE must be the same as the remote service ID specified on the other PE.

You can configure routing policies in cross-connect group EVPN instance view. An import routing policy is used for filtering the BGP EVPN routes received by the EVPN instance, and an export routing policy is used for filtering the BGP EVPN routes advertised by the EVPN instance.

Restrictions and guidelines

To modify an EVPN PW, first use the **undo evpn local-service-id remote-service-id** command to delete the original EVPN PW.

Procedure

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Create an EVPN instance for the cross-connect group and enter its view.
evpn encapsulation mpls
4. Configure an RD for the EVPN instance.
route-distinguisher *route-distinguisher*
By default, no RD is configured for the EVPN instance of a cross-connect group.
5. Configure route targets for the EVPN instance.
vpn-target { *vpn-target*<1-8> } [**both** | **export-extcommunity** | **import-extcommunity**]
By default, no route targets are configured for the EVPN instance of a cross-connect group.
Make sure the following requirements are met:

- The import targets of the EVPN instance of a cross-connect group do not match the export targets of a VPN instance, the public instance, or the EVPN instance of a VSI.
 - The export targets of the EVPN instance of a cross-connect group do not match the import targets of a VPN instance, the public instance, or the EVPN instance of a VSI.
6. (Optional.) Apply an export routing policy to the EVPN instance.
export route-policy *route-policy*
 By default, no export routing policy is applied to an EVPN instance.
 7. (Optional.) Apply an import routing policy to the EVPN instance.
import route-policy *route-policy*
 By default, no import routing policy is applied to an EVPN instance.
 8. Return to cross-connect group view.
quit
 9. Enter cross-connect view.
connection *connection-name*
 10. (Optional.) Set an MTU for the PW.
mtu *size*
 The default MTU is 1500 bytes.
 11. Configure an EVPN PW and enter its view.
evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
 [**tunnel-policy** *tunnel-policy-name*] [**pw-class** *class-name*]
 Do not use this command together with the **peer** command for a cross-connect.

Mapping an AC to a cross-connect

About mapping an AC to a cross-connect

After you map a Layer 3 interface or Ethernet service instance to a cross-connect, packets received from the mapped AC are forwarded to the PW or another AC bound to the cross-connect.

When you map an AC to a cross-connect, you can associate Track with the AC. Then, the AC is up only when one or more of the associated track entries are positive.

Restrictions and guidelines for mapping an AC to a cross-connect

This task is mutually exclusive with Ethernet link aggregation. If a Layer 2 or Layer 3 Ethernet interface has been added to a link aggregation group, you cannot map the Layer 3 interface or an Ethernet service instance on the Layer 2 interface to a cross-connect, and vice versa.

Mapping a Layer 3 interface to a cross-connect

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter cross-connect view.

connection *connection-name*

4. Map a Layer 3 interface to the cross-connect.

ac interface *interface-type interface-number* [**access-mode** { **ethernet** | **vlan** }]
[**track** *track-entry-number*&<1-3>]

By default, no Layer 3 interface is bound to the cross-connect.

Configuring EVPN VPWS multihoming

Restrictions and guidelines for EVPN VPWS multihoming

You must configure the same local and remote service IDs on the redundant PEs at a multihomed site.

As a best practice, set the same redundancy mode on the interfaces that act as ACs or are configured with ACs on the redundant PEs at a multihomed site.

You can assign ESIs to a main interface and its subinterfaces.

- If you assign an ESI to a subinterface, the subinterface-specific ESI and ES configuration take precedence over those configured on the main interface. The ES configuration includes the following:
 - **evpn redundancy-mode**.
 - **evpn df-election algorithm**.
 - **evpn df-election preference**.
 - **evpn df-election preference non-revertive**.
 - **evpn timer es-delay**.
- If you do not assign an ESI to a subinterface, it inherits the ESI and ES configuration (if configured) of the main interface. In this scenario, the ES configuration on the subinterface does not take effect.

If you set up an EVPN PW with a redundant PE at the local site, the device uses the BFD configuration in the PW class specified in the **evpn local-service-id remote-service-id** command.
- If the EVPN PW is a primary EVPN PW, the device establishes a dynamic BFD session for the EVPN PW.
- If the EVPN PW is a backup or ECMP EVPN PW, the device does not establish a dynamic BFD session for the EVPN PW.

Assigning an ESI to an interface

About this task

An ESI uniquely identifies an ES. The links on interfaces with the same ESI belong to the same ES. Traffic of the ES can be distributed among the links for load sharing.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
 - Enter Layer 2 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*

- Enter Layer 3 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.
interface route-aggregation *interface-number*
3. Assign an ESI to the interface.
esi *esi-id*
- By default, no ESI is assigned to an interface.

Configuring the DF election algorithm

About this task

At a multihomed EVPN network site, you can modify the DF election algorithm to control the DF election result.

Restrictions and guidelines

You can configure the DF election algorithm in system view and in interface view. The global DF election algorithm takes effect on all ESS, and the interface-specific DF election algorithm takes effect only on the ESS on an interface. The interface-specific DF election algorithm takes precedence over the global DF election algorithm.

Configuring the DF election algorithm globally

1. Enter system view.
system-view
 2. Configure the DF election algorithm.
evpn df-election algorithm *algorithm*
- By default, the VLAN tag-based algorithm is used for DF election.

Configuring the DF election algorithm on an interface

1. Enter system view.
system-view
 2. Enter interface view.
 - Enter Layer 2 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*
 - Enter Layer 3 Ethernet interface view.
interface *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.
interface route-aggregation *interface-number*
 3. Configure the DF election algorithm.
evpn df-election algorithm *algorithm*
- By default, the DF election algorithm specified in system view takes effect.

Configuring preference-based DF election

1. Enter system view.
system-view
2. Enter interface view.
 - o Enter Layer 2 Ethernet interface view.
interface *interface-type interface-number*
 - o Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*
 - o Enter Layer 3 Ethernet interface view.
interface *interface-type interface-number*
 - o Enter Layer 3 aggregate interface view.
interface route-aggregation *interface-number*
3. Set the DF election preference.
evpn df-election preference *preference*
By default, the DF election preference is 32767.
The larger the value, the higher the preference.
4. (Optional.) Enable non-revertive mode for preference-based DF election.
evpn df-election preference non-revertive
By default, non-revertive mode is disabled for preference-based DF election.

Setting the redundancy mode on an interface

About this task

EVPN VPWS multihoming provides the single-active redundancy mode and all-active redundancy mode.

The redundant PEs at a dualhomed site each establish an EVPN PW to a remote PE. To use one PW as a backup of the other PW, use the single-active mode. To distribute traffic across the PWs for load sharing, use the all-active mode.

Restrictions and guidelines

When you configure S-Trunk on the redundant PEs at a dualhomed site, follow these restrictions:

- In single-active redundancy mode, execute the **s-trunk port-role auto** command on the PEs.
- In all-active redundancy mode, execute the **s-trunk port-role primary** command on the PEs.

For more information about S-Trunk, see *High Availability Configuration Guide*.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
 - o Enter Layer 2 Ethernet interface view.
interface *interface-type interface-number*
 - o Enter Layer 2 aggregate interface view.
interface bridge-aggregation *interface-number*
 - o Enter Layer 3 Ethernet interface view.

- interface** *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.
 - interface route-aggregation** *interface-number*
 - 3. Set the redundancy mode.
- evpn redundancy-mode** { **all-active** | **single-active** }
- By default, the all-active redundancy mode is used.

Setting the DF election delay

About this task

The DF election can be triggered by site-facing interface status changes, redundant PE membership changes, and interface ESI changes. To prevent frequent DF elections from degrading network performance, set the DF election delay. The DF election delay defines the minimum interval allowed between two DF elections.

Procedure

1. Enter system view.
- system-view**
2. Set the DF election delay.
- evpn multihoming timer df-delay** *delay-value*
- By default, the DF election delay is 3 seconds.

Disabling advertisement of EVPN multihoming routes

About this task

EVPN multihoming routes include Ethernet auto-discovery routes and Ethernet segment routes.

In a multihomed EVPN network, perform this task on a redundant PE before you reboot it. This operation allows other PEs to refresh their EVPN routing table to prevent traffic interruption caused by the reboot.

Procedure

1. Enter system view.
- system-view**
2. Disable advertisement of EVPN multihoming routes and withdraw the EVPN multihoming routes that have been advertised to remote sites.
- evpn multihoming advertise disable**
- By default, the device advertises EVPN multihoming routes.

Enabling the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes

About this task

This task enables the device to withdraw the Ethernet auto-discovery routes and MAC/IP advertisement routes that have been advertised, set their Ethernet tag field to 0, and then re-advertise them.

After you configure ESIs for ACs on the redundant edge devices at a dualhomed site, the edge devices advertise Ethernet auto-discovery routes and MAC/IP advertisement routes that carry Ethernet tags. If the remote peers are unable to identify Ethernet tags, you must perform this task on the redundant edge devices to enable communication with the peers.

Restrictions and guidelines

After you assign an ESI to a Layer 3 main interface, its subinterfaces inherit the ESI if they do not have one. In addition, you must map two subinterfaces to different VSIs if the subinterfaces have the same ESI.

Procedure

1. Enter system view.

system-view

2. Enable the device to ignore the Ethernet tag when advertising Ethernet auto-discovery routes and MAC/IP advertisement routes.

evpn multihoming advertise ignore-ethernet-tag

By default, the device advertises Ethernet auto-discovery routes and MAC/IP advertisement routes that carry Ethernet tags.

Enabling the device to monitor the BGP peer status of another local edge device

About this task

Perform this task on the CE-facing interfaces of the edge devices multihomed to a site to prevent device reboots from causing inter-site forwarding failure.

This task excludes unavailable edge devices from DF election at a multihomed site. After an edge device recovers from failure and brings up its CE-facing interface, it starts the advertisement delay timer for Ethernet segment routes and checks the status of the BGP peer specified in the **evpn track peer** command. If the BGP peer comes up before the timer expires, the edge device advertises Ethernet segment routes to the peer. If the BGP peer is still down when the timer expires, the edge device does not advertise Ethernet segment routes to the peer. The edge devices then perform DF election based on the Ethernet segment routes they have received.

Procedure

1. Enter system view.

system-view

2. Enter interface view.

- Enter Layer 2 Ethernet interface view.

interface *interface-type interface-number*

- Enter Layer 2 aggregate interface view.

- interface bridge-aggregation** *interface-number*
 - Enter Layer 3 Ethernet interface view.
 - interface** *interface-type interface-number*
 - Enter Layer 3 aggregate interface view.
 - interface route-aggregation** *interface-number*
- 3. Enable the device to monitor the BGP peer status of another local edge device.
evpn track peer *peer-address*
 By default, the device does not monitor the BGP peer status of the other edge devices at a multihomed site.
- 4. Set the advertisement delay timer for Ethernet segment routes.
evpn timer es-delay *delay-time*
 By default, advertisement of Ethernet segment routes is not delayed.

Configuring FRR for EVPN VPWS

Configuring local FRR

About this task

Local FRR enables two PEs at a multihomed EVPN VPWS network site to set up a bypass PW between them. This feature helps reduce the traffic loss caused by AC failure.

Restrictions and guidelines

On an EVPN instance, EVPN instance-specific local FRR configuration takes precedence over global local FRR configuration.

If you have executed the **evpn frr local enable** command on an EVPN instance, the **undo evpn multihoming vpws-frr local** command does not delete the bypass PW of the EVPN instance.

Enabling local FRR globally

1. Enter system view.
system-view
2. Enable local FRR globally.
evpn multihoming vpws-frr local
 By default, local FRR is disabled globally.

Configuring local FRR on an EVPN instance

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter EVPN instance view.
evpn encapsulation mpls
4. Configure local FRR.

evpn frr local { disable | enable }

By default, an EVPN instance uses the global local FRR configuration of EVPN VPWS.

Configuring remote FRR

About this task

Remote FRR enables two PEs on an EVPN VPWS network to set up a primary PW and a backup PW between them to ensure high availability. The PEs use the primary PW to forward traffic as long as it is available. When the primary PW fails, the PEs switch traffic to the backup PW.

Restrictions and guidelines

On an EVPN instance, EVPN instance-specific remote FRR configuration takes precedence over global remote FRR configuration.

If you have executed the **evpn frr remote enable** command on an EVPN instance, the **undo evpn vpws-frr remote** command does not delete the backup PWs of the EVPN instance.

Enabling remote FRR globally

1. Enter system view.
system-view
2. Enable remote FRR globally.
evpn vpws-frr remote
By default, remote FRR is disabled globally.

Configuring remote FRR on an EVPN instance

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter EVPN instance view.
evpn encapsulation mpls
4. Configure remote FRR.
evpn frr remote { disable | enable }
By default, an EVPN instance uses the global remote FRR configuration of EVPN VPWS.

Configuring LDP or static PWs as ACs for EVPN PWs

About LDP or static PW AC configuration for EVPN PWs

Use this feature for a VPWS network and an EVPN VPWS network to communicate with each other.

Restrictions and guidelines for LDP or static PW AC configuration for EVPN PWs

As a best practice, set the same redundancy mode for the UPWs that use the same ESI at a multihomed site.

You must configure the same local and remote service IDs on the PEs multihomed to the same site.

If the all-active redundancy mode is used at a multihomed site, you must enable the dual receive feature for PW redundancy on the multihomed PEs. To enable this feature, use the **protection dual-receive** command.

Prerequisites for LDP or static PW AC configuration for EVPN PWs

Perform the following tasks:

- In the VPWS network, configure VPWS settings on the PEs and set up LDP or static PWs.
- In the EVPN VPWS network, configure EVPN VPWS settings on the PEs and set up EVPN PWs.

Configuring an LDP PW as an AC for an EVPN PW

Restrictions and guidelines

The data encapsulation type of an LDP PW must be the same as the access mode of the ACs mapped to the same VSI as the LDP PW. If they are different, perform one of the following tasks:

- Use the **pw-type** command on the PW class to which the LDP PW belongs to change the PW data encapsulation type.
- Use the **xconnect vsi** command on the ACs and specify the **access-mode** parameter in the command to change the access mode of the ACs.

Procedure

1. Enter system view.
system-view
2. Enter cross-connect group view.
xconnect-group *group-name*
3. Enter EVPN instance view of a cross-connect group.
evpn encapsulation mpls
4. Return to cross-connect group view.
quit
5. Enter cross-connect view.
connection *connection-name*
6. Configure an LDP PW and enter cross-connect PW view.
peer *ip-address* **pw-id** *pw-id* [**ignore-standby-state**] [**admin** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.
7. (Optional.) Assign an ESI to the UPW.
esi *esi-id*

By default, no ESI is assigned to a PW.

In a multihoming scenario, execute this command on the border PEs that interconnect the VPWS and EVPN VPWS networks.

For more information about this command, see *EVPN Command Reference*.

8. (Optional.) Set the redundancy mode for the UPW.

evpn redundancy-mode { **all-active** | **single-active** }

By default, the all-active redundancy mode is used.

In a multihoming scenario, execute this command on the border PEs that interconnect the VPWS and EVPN VPWS networks.

For more information about this command, see *EVPN Command Reference*.

9. Configure a backup LDP PW and enter cross-connect PW view.

backup-peer *ip-address* **pw-id** *pw-id* [**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

In a multihoming scenario, execute this command on a PE multihomed to the border PEs that interconnect the VPWS and EVPN VPWS networks.

10. Return to cross-connect view.

quit

quit

11. Create an EVPN PW and enter its view.

evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
[**tunnel-policy** *tunnel-policy-name*] [**pw-class** *class-name*]

Do not use this command together with the **peer** command in cross-connect view.

Configuring a static PW as an AC for an EVPN PW

1. Enter system view.

system-view

2. Enter cross-connect group view.

xconnect-group *group-name*

3. Enter EVPN instance view of a cross-connect group.

evpn encapsulation mpls

4. Return to cross-connect group view.

quit

5. Enter cross-connect view.

connection *connection-name*

6. Configure a static PW and enter cross-connect PW view.

peer *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value* [**admin** | **pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

For more information about this command, see MPLS L2VPN commands in *MPLS Command Reference*.

7. (Optional.) Assign an ESI to the UPW.

esi *esi-id*

By default, no ESI is assigned to a PW.

In a multihoming scenario, execute this command on the border PEs that interconnect the VPWS and EVPN VPWS networks.

For more information about this command, see *EVPN Command Reference*.

8. (Optional.) Set the redundancy mode for the UPW.

evpn redundancy-mode { **all-active** | **single-active** }

By default, the all-active redundancy mode is used.

In a multihoming scenario, execute this command on the border PEs that interconnect the VPWS and EVPN VPWS networks.

For more information about this command, see *EVPN Command Reference*.

9. Configure a backup static PW and enter cross-connect PW view.

backup-peer *ip-address* **pw-id** *pw-id* **in-label** *label-value* **out-label** *label-value*
[**pw-class** *class-name* | **tunnel-policy** *tunnel-policy-name*] *

In a multihoming scenario, execute this command on a PE multihomed to the border PEs that interconnect the VPWS and EVPN VPWS networks.

10. Return to cross-connect view.

quit

quit

11. Create an EVPN PW and enter its view.

evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*
[**tunnel-policy** *tunnel-policy-name*] [**pw-class** *class-name*]

Do not use this command together with the **peer** command in cross-connect view.

Display and maintenance commands for EVPN VPWS

Execute **display** commands in any view and **reset** commands in user view.

For more information about the following BGP commands, see *Layer 3—IP Routing Command Reference*:

- **display bgp group.**
- **display bgp peer.**
- **display bgp update-group.**

For more information about the following MPLS L2VPN commands, see *MPLS Command Reference*:

- **display l2vpn forwarding.**
- **display l2vpn interface.**
- **display l2vpn pw.**
- **display l2vpn pw-class.**
- **reset l2vpn statistics ac.**
- **reset l2vpn statistics pw.**

For more information about the **display l2vpn pw bfd** command, see MPLS OAM commands in *MPLS Command Reference*.

Task	Command
Display BGP peer group information.	display bgp [instance <i>instance-name</i>] group l2vpn evpn [group-name <i>group-name</i>]

Task	Command
Display BGP peer or peer group information.	display bgp [<i>instance instance-name</i>] peer l2vpn evpn [<i>ipv4-address mask-length</i> { <i>ipv4-address</i> group-name group-name } log-info [<i>ipv4-address</i>] verbose]
Display information about BGP update groups.	display bgp [<i>instance instance-name</i>] update-group l2vpn evpn [<i>ipv4-address</i>]
Display BGP EVPN routes.	display bgp [<i>instance instance-name</i>] l2vpn evpn [peer { <i>ipv4-address</i> <i>ipv6-address</i> } { advertised-routes received-routes } [statistics] route-distinguisher route-distinguisher [route-type { auto-discovery es mac-ip }] [{ <i>evpn-route route-length</i> <i>evpn-prefix</i> } [advertise-info]] route-type { auto-discovery es mac-ip } statistics]
Display information about peers that are automatically discovered through BGP.	display evpn auto-discovery { { imet mac-ip } [mpls] [peer ip-address] macip-prefix [nexthop next-hop] [count] }
Display DF election information.	display evpn df-election [xconnect-group group-name] [esi esi-id]
Display EVPN ES information.	display evpn es { local [count [xconnect-group group-name] [esi esi-id] [verbose]] remote [xconnect-group group-name] [esi esi-id] [nexthop next-hop] [verbose] }
Display EVPN instance information.	display evpn instance [xconnect-group group-name] [verbose]
Display EVPN routing table information.	display evpn routing-table { public-instance vpn-instance vpn-instance-name } [count]
Display cross-connect forwarding information.	In standalone mode: display l2vpn forwarding { ac pw } [xconnect-group group-name] [verbose] In IRF mode: display l2vpn forwarding { ac pw } [xconnect-group group-name] [slot slot-number] [verbose]
Display L2VPN information for Layer 3 interfaces mapped to cross-connects.	display l2vpn interface [xconnect-group group-name <i>interface-type interface-number</i>] [verbose]
Display L2VPN PW information.	display l2vpn pw [xconnect-group group-name] [protocol { bgp evpn ldp static }] [verbose]
Display BFD information for PWs.	display l2vpn pw bfd [peer peer-ip remote-service-id <i>remote-service-id</i>]
Display PW class information.	display l2vpn pw-class [<i>class-name</i>]
Display EVPN information about cross-connects.	display evpn route xconnect-group [name group-name [connection connection-name]]

Task	Command
	[count]

Command reference

EVPN VPWS shares some commands with EVPN VPLS. For more information, see EVPN VPLS commands.

ac interface

Use **ac interface** to map an interface to a cross-connect.

Use **undo ac interface** to delete the mapping between a cross-connect and an interface.

Syntax

ac interface *interface-type interface-number* [**access-mode** { **ethernet** | **vlan** }] [**track** *track-entry-number*&<1-3>]

undo ac interface *interface-type interface-number*

Default

No interface is mapped to a cross-connect.

Views

Cross-connect view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

access-mode: Specifies an access mode. The default access mode varies by AC type.

- If the AC is a Layer 3 interface or subinterface, the default access mode is as follows:
 - For a VLAN interface, the default access mode is VLAN. For a Layer 3 interface of another type, the default access mode is Ethernet.
 - For a Layer 3 subinterface, the default access mode is VLAN.

ethernet: Specifies the Ethernet access mode.

vlan: Specifies the VLAN access mode.

track *track-entry-number*&<1-3>: Specifies a space-separated list of up to three track entry numbers in the range of 1 to 1024. The AC is up only if a minimum of one associated track entry is in positive state.

Usage guidelines

After you execute this command, packets received from the mapped Layer 3 interface are forwarded to the PW or another AC bound to the cross-connect.

The access mode determines how the PE treats the VLAN tag in Ethernet frames received from the AC. It also determines how the PE forwards Ethernet frames out of the AC.

- **VLAN access mode**—Ethernet frames received from the AC must carry a VLAN tag in the Ethernet header. The VLAN tag is called a P-tag, which is assigned by the service provider. Ethernet frames sent out of the AC must also carry the P-tag.

- **Ethernet access mode**—If Ethernet frames from the AC have a VLAN tag in the header, the VLAN tag is called a U-tag, and the PE ignores it. Ethernet frames sent out of the AC do not carry the P-tag.

Examples

```
# Map GigabitEthernet 1/0/1 to cross-connect aaa in cross-connect group vpna.
[Sysname] xconnect-group vpna
[Sysname-xcg-vpna] connection aaa
[Sysname-xcg-vpna-aaa] ac interface gigabitethernet 1/0/1
```

Related commands

connection (*MPLS Command Reference*)
display l2vpn interface (*MPLS Command Reference*)
display l2vpn service-instance (*MPLS Command Reference*)
pw-type (*MPLS Command Reference*)

display evpn route xconnect-group

Use **display evpn route xconnect-group** to display EVPN information about cross-connects.

Syntax

```
display evpn route xconnect-group [ name group-name [ connection connection-name ] ]
[ count ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

name *group-name*: Specifies a cross-connect group by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a cross-connect group, this command displays EVPN information about all cross-connect groups.

connection *connection-name*: Specifies a cross-connect by its name, a case-sensitive string of 1 to 20 characters excluding hyphens (-). If you do not specify a cross-connect, this command displays EVPN information about all cross-connects in the specified cross-connect group.

count: Displays the number of EVPN cross-connects. If you do not specify this keyword, the command displays detailed EVPN information.

Usage guidelines

If you do not specify any parameters, this command displays detailed EVPN information about all cross-connects.

Examples

```
# Display detailed EVPN information about all cross-connects.
<Sysname> display evpn route xconnect-group

Ctrl Flags: P - Primary, B - Backup, C - Control word

Xconnect group name: aa
Connection name: aaa
Encapsulation      : MPLS
```

```

ESI : 0001.0002.0002.0002.0002
Local service ID : 16777215
Remote service ID : 16777214
Control word : Enabled
In label : 502
Local MTU : 1500
AC state : Up
Tunnel policy : -
PW class : -
PW type : VLAN

```

Nexthop	ESI	Out label	Flags	MTU	State
192.123.123.123	0001.0002.0002.0002.0001	1299	PC	1500	Up
192.1.1.1	0001.0002.0002.0002.0001	1026	B	1500	Down

Connection name: aab

```

Encapsulation : MPLS
ESI : 0000.0000.0000.0000.0000
Local service ID : 1
Remote service ID : 2
Control word : Disabled
In label : 323
Local MTU : 1500
AC state : Up
Tunnel policy : -
PW class : -
PW type : VLAN

```

Nexthop	ESI	Out label	Flags	MTU	State
192.1.1.1	0002.0002.0002.0002.0001	1234	P	1500	Up
192.2.1.2	0002.0002.0002.0002.0001	603	P	1500	Up

Connection name: aac

```

Encapsulation : MPLS
ESI : 0000.0000.0000.0000.0000
Local service ID : 3
Remote service ID : 4
Control word : Enabled
In label : -
Local MTU : 1500
AC state : Up
Tunnel policy : -
PW class : -
PW type : Ethernet

```

Nexthop	ESI	Out label	Flags	MTU	State
192.1.1.3	0000.0000.0000.0000.0000	555	P	1500	Idle

Xconnect group name: vpna

Connection name: pw1

```

Encapsulation : SRv6

```

```

ESI : 0000.0000.0000.0000.0000
Local service ID : 1
Remote service ID : 2
In SID[DX2] : 100::1
In SID[DX2L] : -
Local MTU : 1500
AC State : Up
Tunnel policy : -
PW class : -
PW type : Ethernet
SRv6 Tunnel:
  Next Hop : 2::2
  ESI : 0000.0000.0000.0000.0000
  Out SID : 200::1
  Flags : P
  MTU : 1500
  State : Up

```

Display the total number of EVPN cross-connects.

```
<Sysname> display evpn route xconnect-group count
```

Total number of entries: 2

Table 95 Command output

Field	Description
Xconnect group name	Cross-connect group name.
Connection name	Cross-connect name.
Encapsulation	EVPN encapsulation type: • VXLAN. • MPLS. • SRv6.
In label	PW incoming label.
Local MTU	Local MTU in bytes.
AC state	AC state: • Up. • Down. This field displays a hyphen (-) if no AC is configured.
PW type	PW data encapsulation type: • Ethernet. • VLAN.
Nexthop	Remote PE address.
Out label	PW outgoing label.
Flags	PW attribute flags: • P—The received route has the primary flag. A primary PW needs to be set up. • B—The received route has the backup flag. A backup PW needs to be set up. • C—The received route has the control word flag, which indicates that control word is enabled on the peer. For the EVPN PWs to

Field	Description
	come up, you must enable control word on the local device.
MTU	MTU in the received route, in bytes.
State	EVPN PW state: • Up. • Down. • Idle—The incoming or outgoing label is not available.
In SID[DX2]	Incoming End.DX2 SID.
In SID[DX2L]	Incoming End.DX2L SID.
Out SID	Outgoing SID.

evpn frr local (cross-connect group EVPN instance view)

Use **evpn frr local enable** to enable local fast reroute (FRR) on an EVPN instance.

Use **evpn frr local disable** to disable local FRR on an EVPN instance and delete the existing bypass PW.

undo evpn frr local to restore the default.

Syntax

evpn frr local { disable | enable }

undo evpn frr local

Default

An EVPN instance uses the global local FRR configuration of EVPN VPWS.

Views

Cross-connect group EVPN instance view

Predefined user roles

network-admin

Usage guidelines

Local FRR enables two PEs at a multihomed EVPN VPWS network site to set up a bypass PW between them. This feature helps reduce the traffic loss caused by AC failure.

At a multihomed EVPN VPWS network site, CE 1 is dualhomed to PE 1 and PE 2, and PE 1 is the DF. When the AC on PE 1 fails, PE 1 advertises the local unreachable event to PE 2 and remote PEs for the remote PEs to switch traffic to the PWs to PE 2. In this situation, PE 1 drops the packets that the remote PEs send before they are notified of the local unreachable event. To resolve this issue, enable local FRR on PE 1 and PE 2. When receiving packets from the remote PEs after its AC fails, PE 1 forwards the packets to PE 2 over the bypass PW to prevent traffic loss.

On an EVPN instance, EVPN instance-specific local FRR configuration takes precedence over global local FRR configuration.

Examples

Enable local FRR on the EVPN instance of cross-connect group **aa**.

```
<Sysname> system-view
[Sysname] xconnect-group aa
[Sysname-xcg-1] evpn encapsulation mpls
```

```
[Sysname-xcg-1-evpn-mpls] evpn frr local enable
```

Related commands

evpn multihoming vpws-frr local

evpn frr remote

Use **evpn frr remote enable** to enable remote FRR on an EVPN instance.

Use **evpn frr remote disable** to disable remote FRR on an EVPN instance and delete existing backup PWs.

Use **undo evpn frr remote** to restore the default.

Syntax

evpn frr remote [**disable** | **enable**]

undo evpn frr remote

Default

An EVPN instance uses the global remote FRR configuration of EVPN VPWS.

Views

Cross-connect group EVPN instance view

Predefined user roles

network-admin

Usage guidelines

Remote FRR enables two PEs on an EVPN VPWS network to set up a primary PW and a backup PW between them to ensure high availability. The PEs use the primary PW to forward traffic as long as it is available. When the primary PW fails, the PEs switch traffic to the backup PW.

Remote FRR is supported only cross-connect group EVPN instances that use MPLS encapsulation.

On an EVPN instance, EVPN instance-specific remote FRR configuration takes precedence over global remote FRR configuration.

Examples

Enable remote FRR on the EVPN instance of cross-connect group **xcga**.

```
<Sysname> system-view
```

```
[Sysname] xconnect-group xcga
```

```
[Sysname-xcg-xcga] evpn encapsulation mpls
```

```
[Sysname-xcg-xcga-evpn-mpls] evpn frr remote enable
```

Related commands

evpn vpws-frr remote

evpn local-service-id remote-service-id

Use **evpn local-service-id remote-service-id** to create an EVPN PW and enter its view, or enter the view of an existing EVPN PW.

Use **undo evpn local-service-id remote-service-id** to delete an EVPN PW.

Syntax

evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id* [**tunnel-policy** *tunnel-policy-name*] [**pw-class** *class-name*]

undo evpn local-service-id *local-service-id* **remote-service-id** *remote-service-id*

Default

No EVPN PWs exist.

Views

Cross-connect view

Predefined user roles

network-admin

Parameters

local-service-id: Specifies a local service ID in the range of 1 to 16777215.

remote-service-id: Specifies a remote service ID in the range of 1 to 16777215.

tunnel-policy *tunnel-policy-name*: Specifies a tunnel policy by its name, a case-sensitive string of 1 to 19 characters. If you do not specify a tunnel policy, the PW uses the default tunnel policy.

pw-class *class-name*: Specifies a PW class by its name, a case-sensitive string of 1 to 19 characters. You can specify a PW class to configure the PW data encapsulation type and control word for the PW. If you do not specify a PW class, the PW data encapsulation type is determined by the link type of the interface. The control word feature is not supported for PW data encapsulation types that do not require using control word.

Usage guidelines

You can use the **evpn local-service-id remote-service-id** command to concatenate two EVPN PWs on the same cross-connect.

To modify an EVPN PW, first use the **undo evpn local-service-id remote-service-id** command to delete the original EVPN PW.

If you set up an EVPN PW with a redundant PE at the local site, the device uses the BFD configuration in the PW class specified in the **evpn local-service-id remote-service-id** command.

- If the EVPN PW is a primary EVPN PW, the device establishes a dynamic BFD session for the EVPN PW.
- If the EVPN PW is a backup or ECMP EVPN PW, the device does not establish a dynamic BFD session for the EVPN PW.

Examples

Create an EVPN PW and enter its view, and specify tunnel policy **aaa** and PW class **bbb** for it.

```
<Sysname> system-view
```

```
[Sysname] xconnect-group aaa
```

```
[Sysname-xcg-aaa] connection ac2pw
```

```
[Sysname-xcg-aaa-ac2pw] evpn local-service-id 2 remote-service-id 4 tunnel-policy aaa  
pw-class bbb
```

```
[Sysname-xcg-aaa-ac2pw-2-4]
```

evpn multihoming vpws-frr local

Use **evpn multihoming vpws-frr local** to enable local FRR globally for EVPN VPWS.

Use **undo evpn multihoming vpws-frr local** to disable local FRR globally for EVPN VPWS and delete existing bypass PWs.

Syntax

evpn multihoming vpws-frr local

undo evpn multihoming vpws-frr local

Default

Local FRR is disabled globally for EVPN VPWS.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Local FRR enables two PEs at a multihomed EVPN VPWS network site to set up a bypass PW between them. This feature helps reduce the traffic loss caused by AC failure.

At a multihomed EVPN VPWS network site, CE 1 is dualhomed to PE 1 and PE 2, and PE 1 is the DF. When the AC on PE 1 fails, PE 1 advertises the local unreachable event to PE 2 and remote PEs for the remote PEs to switch traffic to the PWs to PE 2. In this situation, PE 1 drops the packets that the remote PEs send before they are notified of the local unreachable event. To resolve this issue, enable local FRR on PE 1 and PE 2. When receiving packets from the remote PEs after its AC fails, PE 1 forwards the packets to PE 2 over the bypass PW to prevent traffic loss.

On an EVPN instance, EVPN instance-specific local FRR configuration takes precedence over global local FRR configuration.

If you have executed the **evpn frr local enable** command on an EVPN instance, the **undo evpn multihoming vpws-frr local** command does not delete the bypass PW of the EVPN instance.

Examples

```
# Enable local FRR globally for EVPN VPWS.
<Sysname> system-view
[Sysname] evpn multihoming vpws-frr local
```

Related commands

evpn frr local (cross-connect group EVPN instance view)

evpn redundancy-mode

Use **evpn redundancy-mode** to set the redundancy mode on an interface or UPW.

Use **undo evpn redundancy-mode** to restore the default.

Syntax

evpn redundancy-mode { all-active | single-active }

undo evpn redundancy-mode

Default

The all-active redundancy mode is used.

Views

Interface view

Cross-connect PW view

VSI LDP PW view

VSI static PW view

Predefined user roles

network-admin

Parameters

single-active: Specifies the single-active mode.

all-active: Specifies the all-active mode.

Usage guidelines

This command is supported only by a multihomed EVPN VPWS, EVPN VPLS, EVPN VPWS over SRv6, or EVPN VPLS over SRv6 network. A multihomed EVPN VXLAN network supports only the all-active mode.

You can set the redundancy mode for a VSI LDP PW or VSI static PW only if you do not specify the **no-split-horizon** keyword when executing the **peer** command for the PW.

The redundant PEs at a dualhomed site each establish an EVPN PW or SRv6 PW to a remote PE. To use one PW as a backup of the other PW, use the single-active mode. To distribute traffic across the PWs for load sharing, use the all-active mode.

As a best practice, set the same redundancy mode on the interfaces or UPWs that act as ACs or are configured with ACs on the redundant PEs at a multihomed site.

Make sure the interface or UPW where you execute this command is assigned an ESI.

Examples

Set the redundancy mode to single-active on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] evpn redundancy-mode single-active
```

Set the redundancy mode to single-active on cross-connect PW 34.

```
<Sysname> system-view
[Sysname] xconnect-group 1
[Sysname-xcg-1] connection 1
[Sysname-xcg-1-1] peer 1.1.1.1 pw-id 34
[Sysname-xcg-1-1-1.1.1.1-34] evpn redundancy-mode single-active
```

Related commands

esi

New feature: EVPN VXLAN forwarding mode

Configuring the traffic forwarding mode for EVPN VXLAN

Restrictions and guidelines

The asymmetric IRB mode is supported only on distributed EVPN gateways. The mode takes effect only on Layer 3 traffic forwarded in the same VXLAN. In addition, the same VSI interface on different distributed EVPN gateways must have different IP addresses.

Procedure

1. Enter system view.

system-view

2. Configure the traffic forwarding mode for EVPN VXLAN. Choose one of the following options:

- o Enable asymmetric IRB mode.

evpn irb asymmetric

- o Enable symmetric IRB mode.

undo evpn irb asymmetric

By default, a distributed EVPN gateway forwards EVPN VXLAN traffic in symmetric IRB mode.

Command reference

evpn irb asymmetric

Use **evpn irb asymmetric** to enable asymmetric IRB for EVPN VXLAN.

Use **undo evpn irb asymmetric** to restore the default.

Syntax

evpn irb asymmetric

undo evpn irb asymmetric

Default

Symmetric IRB is enabled for EVPN VXLAN.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command to set the IRB mode for EVPN VXLAN.

Examples

Enable asymmetric IRB for EVPN VXLAN.

```
<Sysname> system-view
```

```
[Sysname] evpn irb asymmetric
```

New feature: Enabling an ED to replace the L3 VXLAN ID, RD, and route targets of BGP EVPN routes

Enabling an ED to replace the L3 VXLAN ID, RD, and route targets of BGP EVPN routes

About this task

In an EVPN-DCI network, use this feature to hide the L3 VXLAN IDs of data centers or enable communication between data centers that use different L3 VXLAN IDs or route targets.

After you enable this feature on an ED, the ED performs the following operations after receiving BGP EVPN routes:

1. Matches the route targets of the routes with the import route targets of local VPN instances.
2. Replaces the L3 VXLAN ID, RD, and route targets of the routes with those of the matching local VPN instance.
3. Advertises the routes to a VTEP or remote ED.

After you execute the **peer re-originated** command, the ED advertises only reoriginated BGP EVPN routes. For the ED to advertise both original and reoriginated BGP EVPN routes, execute the **peer advertise original-route** command.

An ED configured with the **peer re-originated** and **peer advertise original-route** commands advertises both original and reoriginated BGP EVPN routes. For the ED to advertise only original BGP EVPN routes, execute the **peer suppress re-originated** command on the ED.

Restrictions and guidelines

If the RD of a received BGP EVPN route is identical to the RD of the matching local VPN instance, an ED does not replace the L3 VXLAN ID and route targets of the route or reoriginate the route. As a result, the ED does not advertise the route. As a best practice, assign unique RDs to VPN instances on different EVPN gateways and EDs when you use this feature.

Procedure

1. Enter system view.
system-view
2. Enter BGP instance view.
bgp as-number [instance instance-name]
3. Enter BGP EVPN address family view.
address-family l2vpn evpn
4. Replace the L3 VXLAN ID, RD, and route targets (optional) of received BGP EVPN routes.
peer { group-name | ipv4-address [mask-length] } re-originated [ip-prefix | mac-ip] [replace-rt]

By default, the device does not modify the BGP EVPN routes that are received from peers or peer groups.

5. (Optional.) Enable the device to advertise original BGP EVPN routes together with the reoriginated BGP EVPN routes after the **peer re-originated** command is executed.
peer { group-name | ipv4-address [mask-length] } advertise original-route

By default, the device advertises only reoriginated BGP EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

6. (Optional.) Suppress advertisement of reoriginated BGP EVPN routes to a peer or peer group.

```
peer { group-name | ipv4-address [ mask-length ] } suppress re-originated  
{ ip-prefix | mac-ip }
```

By default, the device advertises reoriginated BGP EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

Command reference

peer advertise original-route

Use **peer advertise original-route** to enable the device to advertise original BGP EVPN routes to a peer or peer group.

Use **undo peer advertise original-route** to disable the device from advertising original BGP EVPN routes to a peer or peer group.

Syntax

```
peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
advertise original-route  
undo peer { group-name | ipv4-address [ mask-length ] | ipv6-address [ prefix-length ] }  
advertise original-route
```

Default

The device advertises reoriginated BGP EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

Views

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must exist.

ipv4-address: Specifies a peer by its IPv4 address. The peer must exist.

mask-length: Specifies a mask length in the range of 0 to 32. To specify a subnet, you must specify both the *ipv4-address* and *mask-length* arguments.

ipv6-address: Specifies a peer by its IPv6 address. The peer must exist.

prefix-length: Specifies a prefix length in the range of 0 to 128. To specify a subnet, you must specify both the *ipv6-address* and *prefix-length* arguments.

Usage guidelines

For this command to take effect on an ED, first execute the **peer re-originated** command.

In an EVPN-DCI network, an ED configured with the **peer re-originated** command advertises only reoriginated BGP EVPN routes. For the ED to advertise both original and reoriginated BGP EVPN routes to a peer or peer group, execute the **peer advertise original-route** command on the ED.

Examples

```
# Enable the device to advertise original BGP EVPN routes to peer 1.1.1.1.
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn evpn
[Sysname-bgp-default-evpn] peer 1.1.1.1 advertise original-route
```

Related commands

peer re-originated

peer suppress re-originated

peer re-originated

Use **peer re-originated** to enable the device to reoriginate BGP EVPN routes based on the BGP EVPN routes received from a peer or peer group.

Use **undo peer re-originated** to disable the device from reoriginating BGP EVPN routes based on the BGP EVPN routes received from a peer or peer group.

Syntax

peer { *group-name* | *ipv4-address* [*mask-length*] } **re-originated** [**ip-prefix** | **mac-ip**] [**replace-rt**]

undo peer { *group-name* | *ipv4-address* [*mask-length*] } **re-originated** [**ip-prefix** | **mac-ip**]

Default

The device does not reoriginate BGP EVPN routes based on received BGP EVPN routes.

Views

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must exist.

ipv4-address: Specifies a peer by its IPv4 address. The peer must exist.

mask-length: Specifies a mask length in the range of 0 to 32. To specify a subnet, you must specify both the *ipv4-address* and *mask-length* arguments.

ip-prefix: Specifies IP prefix advertisement routes.

mac-ip: Specifies MAC/IP advertisement routes.

replace-rt: Replaces the L3 VXLAN ID, RD, and route targets of BGP EVPN routes with those of the matching local VPN instance. If you do not specify this keyword, only the L3 VXLAN ID and RD will be replaced.

Usage guidelines

In an EVPN-DCI network, use this command to hide the L3 VXLAN IDs of data centers or enable communication between data centers that use different L3 VXLAN IDs or route targets.

After you execute this command on an ED, the ED performs the following operations after receiving BGP EVPN routes from a VTEP or remote ED:

1. Matches the route targets of the routes with the import route targets of local VPN instances.
2. Replaces the L3 VXLAN ID, RD, and route targets of the routes with those of the matching local VPN instance.
3. Advertises the routes to a VTEP or remote ED.

After you execute this command, an ED advertises only reoriginated BGP EVPN routes. The original BGP EVPN routes are not advertised.

If the RD of a received BGP EVPN route is identical to the RD of the matching local VPN instance, an ED does not replace the L3 VXLAN ID and route targets of the route or reoriginate the route. As a result, the ED does not advertise the route. As a best practice, assign unique RDs to VPN instances on different EVPN gateways and EDs when you use this command.

If you do not specify the **ip-prefix** or **mac-ip** keyword, this command takes effect on IP prefix advertisement routes.

Examples

Replace the L3 VXLAN ID, RD, and route targets of the IP prefix advertisement routes received from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family l2vpn evpn
[Sysname-bgp-default-evpn] peer 1.1.1.1 re-originated ip-prefix replace-rt
```

Related commands

peer advertise original-route
peer suppress re-originated

peer suppress re-originated

Use **peer suppress re-originated** to suppress advertisement of reoriginated BGP EVPN routes to a peer or peer group.

Use **undo peer suppress re-originated** to disable suppression of reoriginated BGP EVPN route advertisement to a peer or peer group.

Syntax

```
peer { group-name | ipv4-address [ mask-length ] } suppress re-originated { ip-prefix | mac-ip }

undo peer { group-name | ipv4-address [ mask-length ] } suppress re-originated
{ ip-prefix | mac-ip }
```

Default

The device advertises reoriginated BGP EVPN routes to peers and peer groups after the **peer re-originated** command is executed.

Views

BGP EVPN address family view

Predefined user roles

network-admin

Parameters

group-name: Specifies a peer group by its name, a case-sensitive string of 1 to 47 characters. The peer group must exist.

ipv4-address: Specifies a peer by its IPv4 address. The peer must exist.

mask-length: Specifies a mask length in the range of 0 to 32. To specify a subnet, you must specify both the *ipv4-address* and *mask-length* arguments.

ip-prefix: Specifies IP prefix advertisement routes.

mac-ip: Specifies MAC/IP advertisement routes.

Usage guidelines

An ED configured with the **peer re-originated** and **peer advertise original-route** commands advertises both original and reoriginated BGP EVPN routes. For the ED to advertise only original BGP EVPN routes to a peer or peer group, execute the **peer suppress re-originated** command on the ED.

Examples

Suppress advertisement of reoriginated IP prefix advertisement routes to peer 1.1.1.1.

```
<Sysname> system-view
```

```
[Sysname] bgp 100
```

```
[Sysname-bgp-default] address-family l2vpn evpn
```

```
[Sysname-bgp-default-evpn] peer 1.1.1.1 suppress re-originated ip-prefix
```

Related commands

peer advertise original-route

peer re-originated

New feature: Enabling EVPN to advertise VPN routes

Command reference

evpn mpls routing-enable

Use **evpn mpls routing-enable** to enable EVPN to advertise the routes of a VPN instance.

Use **undo evpn mpls routing-enable** to disable EVPN from advertising the routes of a VPN instance.

Syntax

evpn mpls routing-enable

undo evpn mpls routing-enable

Default

EVPN does not advertise the routes of VPN instances.

Views

VPN instance IPv4 address family view

VPN instance IPv6 address family view

Predefined user roles

network-admin

Usage guidelines

This command enables devices to exchange the routes of a VPN instance by using IP prefix advertisement routes with MPLS encapsulation. After you execute this command for a VPN instance, the device advertises the routes of the VPN instance through IP prefix advertisement routes. When receiving IP prefix advertisement routes with MPLS encapsulation, the device adds the routes that belong to the VPN instance to the routing table.

For EVPN to add MPLS encapsulation to IP prefix advertisement routes, you must execute the **peer advertise encap-type mpls** command in BGP EVPN address family view.

Examples

```
# Enable EVPN to advertise the IPv4 routes of VPN instance vpna.
```

```
<Sysname> system-view
```

```
[Sysname] ip vpn-instance vpna
```

```
[Sysname-vpn-instance-vpna] address-family ipv4
```

```
[Sysname-vpn-ipv4-vpna] evpn mpls routing-enable
```

Related commands

peer advertise encap-type mpls

Modified feature: Displaying BGP EVPN route information with the specified prefix

Feature change description

As from this release, you can use the **display bgp l2vpn evpn** command to display BGP EVPN route information with the specified prefix.

Command changes

Modified command: display bgp l2vpn evpn

Old syntax

```
display bgp [ instance instance-name ] l2vpn evpn [ peer { ipv4-address | ipv6-address }  
{ advertised-routes | received-routes } [ statistics ] | route-distinguisher  
route-distinguisher [ route-type { auto-discovery | es | imet | ip-prefix | mac-ip } ]  
[ evpn-route route-length [ advertise-info ] ] | route-type { auto-discovery | es | imet |  
ip-prefix | mac-ip } | statistics ]
```

New syntax

```
display bgp [ instance instance-name ] l2vpn evpn [ peer { ipv4-address | ipv6-address }  
{ advertised-routes | received-routes } [ statistics ] | route-distinguisher  
route-distinguisher [ route-type { auto-discovery | es | imet | ip-prefix | mac-ip } ]  
[ { evpn-route route-length | evpn-prefix } [ advertise-info ] ] | route-type  
{ auto-discovery | es | imet | ip-prefix | mac-ip } | statistics ]
```

Views

Any view

Change description

After modification, this command supports the *evpn-prefix* argument. To display detailed information about a BGP EVPN route, specify this argument. The value for this argument is a case-insensitive string of 1 to 512 characters in *evpn-route/route-length* format.

Modified feature: Saving the configuration in safe mode

Feature change description

As from this release, you can save the configuration in safe mode.

NETCONF message example:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save OverWrite="false" Binary-only="false" Safely="false">
    <file>Configuration file name</file>
  </save>
</rpc>
```

Item	Description
Safely	Determines whether to save the configuration file in safe mode or fast mode. Available values: true—Saves the configuration in safe mode. In this mode, the system saves the configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a disruptive event such as a reboot or power failure occurs during the save operation, the device can still start up with the original next-startup configuration file. false—Saves the configuration in fast mode. In this mode, the system directly overwrites the target next-startup configuration file. If a disruptive event such as a reboot, power failure, out-of-memory, out-of-storage event occurs during this process, the next-startup configuration file is lost. You must specify a new startup configuration file after the device reboots. By default, the Safely attribute is set to false if you do not specify a value for it. Safe mode is slower than fast mode, but more secure. As a best practice, use the safe mode if the power source is not reliable or you are remotely configuring the device.

New feature: Configuring MACsec

About MACsec

Media Access Control Security (MACsec) secures data communication on IEEE 802 LANs. MACsec provides services such as data encryption, frame integrity check, and data origin validation for frames on the MAC sublayer of the Data Link Layer. MACsec usually cooperates with 802.1X authentication to use the keys generated from MACsec Key Agreement (MKA) negotiation for authenticated users' data encryption and integrity check. This collaboration can prevent ports from processing packets from unauthenticated users or tampered packets.

Basic concepts

CA

Connectivity association (CA) is a group of participants that use the same key and key algorithm. The encryption key used by the CA participants is called a connectivity association key (CAK). The following types of CAKs are available:

- **Pairwise CAK**—Used by CAs that have two participants.
- **Group CAK**—Used by CAs that have more than two participants.

The pairwise CAK is used most often because MACsec is typically applied to point-to-point networks.

A CAK can be an encryption key generated during 802.1X authentication or a user-configured preshared key. The user-configured preshared key takes precedence over the 802.1X-generated key.

SA

Secure association (SA) is an agreement negotiated by CA participants. The agreement includes a cipher suite and keys for integrity check.

A secure channel can contain more than one SA. Each SA uses a unique secure association key (SAK). The SAK is generated from the CAK, and MACsec uses the SAK to encrypt data transmitted along the secure channel.

MACsec Key Agreement (MKA) limits the number of packets that can be encrypted by an SAK. When the limit is exceeded, the SAK will be refreshed. For example, when packets with the minimum size are sent on a 10-Gbps link, an SAK rekey occurs about every 300 seconds.

MACsec services

Data encryption

MACsec enables a port to encrypt outbound frames and decrypt MACsec-encrypted inbound frames. The keys for encryption and decryption are negotiated by MKA.

Integrity check

MACsec performs integrity check when the device receives a MACsec-encrypted frame. The integrity check uses the following process:

- Uses a key negotiated by MKA to calculate an integrity check value (ICV) for the frame.
- Compares the calculated ICV with the ICV in the frame trailer.
 - If the ICVs are the same, the device verifies the frame as legal.
 - If the ICVs are different, the device determines whether to drop the frame based on the validation mode. The device supports the following validation modes:
 - **check**—Performs validation only, and does not drop illegal frames.
 - **disabled**—Does not perform validation.
 - **strict**—Performs validation, and drops illegal frames.

Replay protection

When MACsec frames are transmitted over the network, frame disorder might occur. MACsec replay protection allows the device to accept the out-of-order packets within the replay protection window size and drop other out-of-order packets.

MACsec application modes

MACsec supports client-oriented and device-oriented modes.

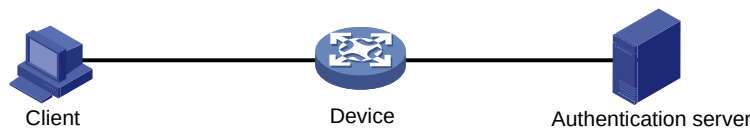
Client-oriented mode

As shown in [Figure 68](#), MACsec secures data transmission between the client and the access device. In this mode, MACsec must operate with 802.1X authentication.

Client-oriented MACsec includes the following entities:

- **Client (supplicant)**—A user terminal seeking access to the LAN. The terminal must have 802.1X software to authenticate to the access device. The terminal also performs CAK negotiation and packet encryption.
- **Access device (authenticator)**—Authenticates the client to control access to the LAN and performs CAK negotiation and packet encryption.
- **Authentication server**—Provides AAA services for the access device. The authentication server is typically a RADIUS server. After the client passes authentication, the authentication server generates and distributes the CAK to the client and the access device.

Figure 68 Client-oriented mode



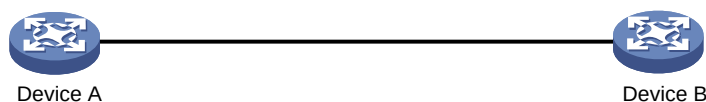
NOTE:

In client-oriented mode, an MKA-enabled port on the access device must perform port-based 802.1X access control. The authentication method must be EAP relay.

Device-oriented mode

As shown in [Figure 69](#), MACsec secures data transmission between devices. In this mode, the devices do not perform identity authentication, and the same preshared key must be configured on the MACsec ports that connect the devices. The devices use the configured preshared key as the CAK.

Figure 69 Device-oriented mode

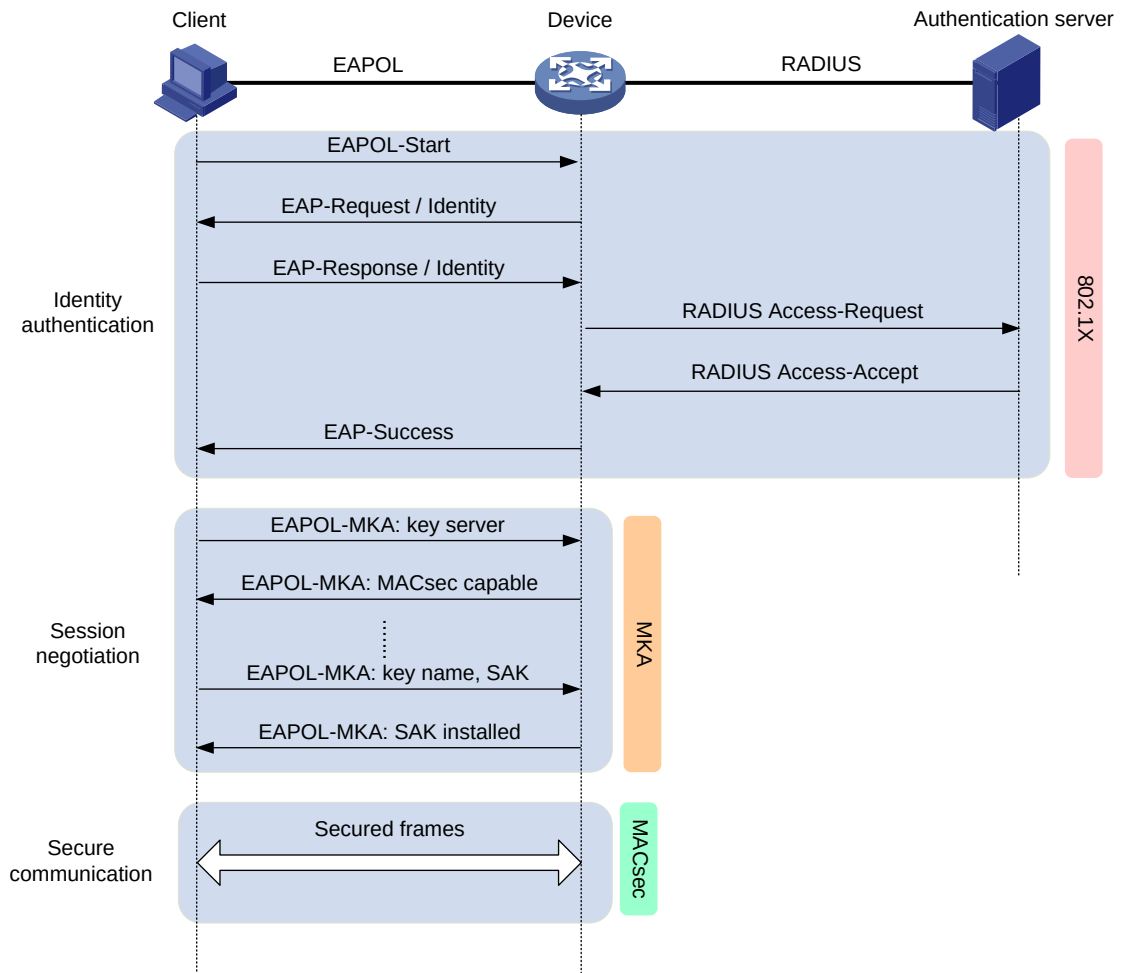


MACsec operating mechanism

Operating mechanism for client-oriented mode

[Figure 70](#) illustrates how MACsec operates in client-oriented mode.

Figure 70 MACsec interactive process in client-oriented mode



The following shows the MACsec process:

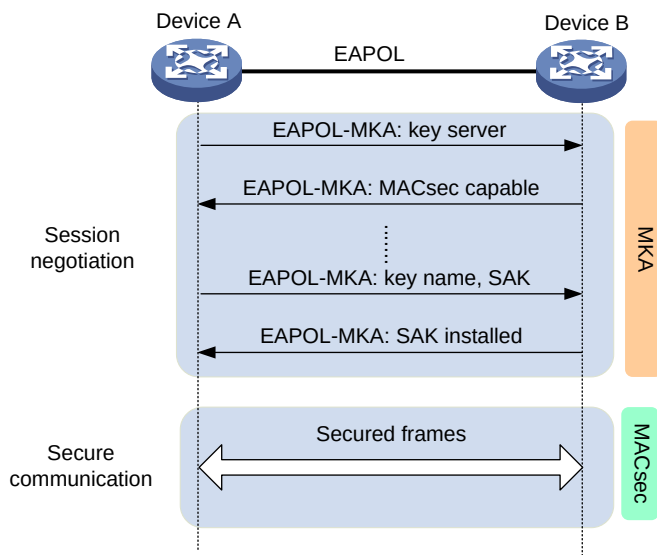
2. After the client passes 802.1X authentication, the RADIUS server distributes the generated CAK to the client and the access device.
3. After receiving the CAK, the client and the access device exchange EAPOL-MKA packets. The client and the access device exchange the MACsec capability and required parameters for session establishment. The parameters include MKA key server priority and MACsec desire. During the negotiation process, the access device automatically becomes the key server. The key server generates an SAK from the CAK for packet encryption, and it distributes the SAK to the client.
4. The client and the access device use the SAK to encrypt packets, and they send and receive the encrypted packets in secure channels.
5. When the access device receives a logoff request from the client, it immediately removes the associated secure session from the port. The remove operation prevents an unauthorized client from using the secure session established by the previous authorized client to access the network.

The MKA protocol also defines a session keepalive timer. If one participant does not receive any MKA packets from the peer after the timer expires, the participant removes the established secure session. The keepalive time is 6 seconds.

Operating mechanism for device-oriented mode

As shown in Figure 71, the devices use the configured preshared keys to start the session negotiation.

Figure 71 MACsec interactive process in device-oriented mode



The following shows the MACsec process:

2. The devices use the configured preshared keys as CAKs to exchange EAPOL-MKA packets. They exchange the MACsec capability and required parameters for session establishment. The parameters include MKA key server priority and MACsec desire. During the negotiation process, the port with higher MKA key server priority becomes the key server. The key server generates and distributes an SAK.
3. The devices each use the SAK to encrypt packets and send and receive the encrypted packets in secure channels.
4. When a device receives a logoff request from the peer, it immediately deletes the associated secure session.

If one participant does not receive any MKA packets from the peer after the session keepalive timer expires, the participant removes the established secure session. The keepalive time is 6 seconds.

Protocols and standards

IEEE 802.1X-2010, *Port-Based Network Access Control*

IEEE 802.1AE-2006, *Media Access Control (MAC) Security*

Restrictions: Hardware compatibility with MACsec

Hardware	MACsec compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No

Hardware	MACsec compatibility
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	MACsec compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	MACsec compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No

Hardware	MACsec compatibility
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	Yes

Hardware	MACsec compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

MACsec tasks at a glance

To configure MACsec, perform the following tasks:

1. [Enabling MKA](#)
2. [Enabling MACsec desire](#)
3. [Specifying the cipher suite for MACsec encryption](#)
4. [Configuring a preshared key](#)
This task is required in device-oriented mode. Do not perform this task in client-oriented mode.
5. (Optional.) [Configuring the MKA key server priority](#)
6. (Optional.) [Setting the MKA life time](#)
7. (Optional.) [Configuring MACsec protection parameters](#)
Choose one of the following tasks:
 - [Configuring MACsec protection parameters in interface view](#)
 - [Configuring MACsec protection parameters by MKA policy](#)
8. (Optional.) [Enabling MKA session logging](#)

Enabling MKA

About this task

MKA establishes and manages MACsec secure channels on a port. It also negotiates keys used by MACsec.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Enable MKA.
mka enable
By default, MKA is disabled on the port.

Enabling MACsec desire

About this task

The MACsec desire feature expects MACsec protection for outbound frames. The key server determines whether MACsec protects the outbound frames.

MACsec protects the outbound frames of a port when the following requirements are met:

- The key server is MACsec capable.
- Both the local participant and its peer are MACsec capable.
- A minimum of one participant is enabled with MACsec desire.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Enable MACsec desire.
macsec desire
By default, the port does not expect MACsec protection for outbound frames.

Specifying the cipher suite for MACsec encryption

About this task

MACsec uses the GCM-AES-128 or GCM-AES-256 cipher suite to encrypt, validate, and decrypt protected data frames.

Restrictions and guidelines

This feature is supported only in device-oriented mode. Do not configure this feature on an 802.1X-enabled port.

Make sure the connected MACsec ports are configured with the same cipher suite. If the ports are configured with different cipher suites, they cannot successfully establish MKA sessions.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Specify the cipher suite for MACsec encryption.
macsec cipher-suite { **gcm-aes-128** | **gcm-aes-256** }
By default, MACsec uses the GCM-AES-128 cipher suite for encryption.

Configuring a preshared key

Restrictions and guidelines

In device-oriented mode, configure a preshared key as the CAK to be used during MKA negotiation. To successfully establish an MKA session between two devices, make sure the connected MACsec ports are configured with the same CAK and CKN.

A user-configured preshared key has higher priority than the 802.1X-generated CAK. To ensure a successful MKA session establishment, do not configure a preshared key in client-oriented mode.

Different cipher suites for MACsec encryption have different requirements for the CKN and CAK configuration.

- The GCM-AES-128 cipher suite requires that the CKN and CAK each must be 32 characters long. If the configured CKN or CAK is not 32 characters long, the system performs the following operations when it runs the cipher suite:
 - Automatically increases the length of the CKN or CAK by zero padding if the CKN or CAK contains less than 32 characters.
 - Uses only the first 32 characters if the CKN or CAK contains more than 32 characters.
- The GCM-AES-256 cipher suite requires that the CKN and CAK each must be 64 characters long. If the configured CKN or CAK contains less than 64 characters, the system automatically increases the length of the CKN or CAK by zero padding when it runs the cipher suite.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Set a preshared key.
mka psk ckn name cak { **cipher** | **simple** } *string*
By default, no MKA preshared key exists.

Configuring the MKA key server priority

Restrictions and guidelines

When you configure the MKA key server priority, follow these restrictions and guidelines:

- In client-oriented mode, the access device port automatically becomes the key server. You do not have to configure the MKA key server priority.
- In device-oriented mode, the port that has higher priority becomes the key server. The lower the priority value, the higher the priority. If a port and its peers have the same priority, MACsec compares the secure

channel identifier (SCI) values on the ports. The port with the lowest SCI value (a combination of MAC address and port ID) becomes the key server.

- A port with priority 255 cannot become the key server. For a successful key server selection, make sure a minimum of one participant's key server priority is not 255.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Set the MKA key server priority.
mka priority *priority-value*
The default setting is 0.

Setting the MKA life time

Restrictions and guidelines

This task is applicable only in device-oriented mode.

Make sure the participants at each end of a secure session have the same MKA life time.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Set the MKA life time.
mka timer mka-life *seconds*
By default, the MKA life time is 6 seconds.

Configuring MACsec protection parameters

About MACsec protection parameters

You can set the following MACsec protection parameters:

- **MACsec confidentiality offset**—Specifies the number of bytes starting from the frame header. MACsec encrypts only the bytes after the offset in a frame. The offset value can be 0, 30, or 50.
- **MACsec replay protection**—Allows a MACsec port to accept a number of out-of-order or repeated inbound frames.
- **MACsec validation**—Allows a port to perform integrity check based on the validation modes.

Restrictions and guidelines for MACsec protection parameter configuration

You can configure MACsec protection parameters either in interface view or through MKA policies.

The use of MKA policies provides a centralized method to configure MACsec protection parameters. When you need to configure the same settings for MACsec protection parameters on multiple ports, you can configure them in an MKA policy and apply the policy to the ports.

If you configure a protection parameter in interface view after applying an MKA policy, the configuration in interface view overwrites the configuration of that parameter in the MKA policy. The other protection parameters in the MKA policy still take effect.

If you apply an MKA policy to a port after configuring protection parameters on the port, the settings in the policy overwrite all protection parameter settings in interface view. The protection parameters not configured in the policy are restored to the default.

Configuring MACsec protection parameters in interface view

1. Enter system view.

system-view

2. Enter interface view.

interface *interface-type interface-number*

3. Set the MACsec confidentiality offset.

macsec confidentiality-offset *offset-value*

The default setting is 0, and the entire frame needs to be encrypted.

MACsec uses the confidentiality offset propagated by the key server.

4. Configure MACsec replay protection:

- a. Enable MACsec replay protection.

macsec replay-protection enable

By default, MACsec replay protection is enabled on the port.

- b. Set the MACsec replay protection window size.

macsec replay-protection window-size *size-value*

The default setting is 0. The device accepts only frames that arrive in the correct order. Out-of-order or duplicated frames will be dropped.

The configured replay protection window size takes effect only when MACsec replay protection is enabled.

5. Set a MACsec validation mode.

macsec validation mode { **check** | **disabled** | **strict** }

The default setting is **check**.

To avoid data loss, use the **display macsec** command to verify that MKA negotiation with the peer device has succeeded before you change the mode to **strict**.

Parameter	Description
check	Verifies incoming frames but does not drop illegal frames.
disabled	Disables MACsec validation for incoming frames.
strict	Verifies incoming frames and drops illegal frames.

Configuring MACsec protection parameters by MKA policy

Restrictions and guidelines

An MKA policy can be applied to a port or multiple ports. When you apply an MKA policy to a port, follow these restrictions and guidelines:

- The settings in the MKA policy overwrite all protection parameter settings configured in interface view. The protection parameters not configured in the policy are restored to the default.
- Any modifications to the MKA policy take effect immediately.
- When you remove an MKA policy application from the port, the MACsec parameter settings on the port restore to the default.
- When you apply a nonexistent MKA policy to the port, the port automatically uses the system-defined MKA policy named **default-policy**. If you create the policy, the policy will be automatically applied to the port.

Procedure

1. Enter system view.

system-view

2. Create an MKA policy and enter its view.

mka policy *policy-name*

By default, a system-defined MKA policy exists. The policy name is **default-policy**.

The settings for parameters in the system-defined policy are the same as the default settings for the parameters on a port.

You cannot delete or modify the system-defined MKA policy.

You can create multiple MKA policies.

3. Set the MACsec confidentiality offset.

confidentiality-offset *offset-value*

The default setting is 0, and the entire frame needs to be encrypted.

MACsec uses the confidentiality offset propagated by the key server.

4. Configure MACsec replay protection:

- a. Enable MACsec replay protection.

replay-protection enable

By default, MACsec replay protection is enabled.

- b. Set the replay protection window size.

replay-protection window-size *size-value*

The default replay protection window size is 0. The device accepts only frames that arrive in the correct order. Out-of-order or duplicated frames will be dropped.

5. Set a MACsec validation mode.

validation mode { **check** | **disabled** | **strict** }

The default setting is **check**.

Parameter	Description
check	Verifies incoming frames but does not drop illegal frames.
disabled	Disables MACsec validation for incoming frames.
strict	Verifies incoming frames and drops illegal frames.

6. Apply an MKA policy:
 - a. Return to system view.
quit
 - b. Enter interface view.
interface *interface-type interface-number*
 - c. Apply the MKA policy to the port.
mka apply policy *policy-name*

By default, no MKA policy is applied to a port.

Enabling MKA session logging

About this task

This feature enables the device to generate logs for MKA session changes, such as peer aging and SAK updates. The logs are sent to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Restrictions and guidelines

As a best practice, disable this feature to prevent excessive MKA session log output.

Procedure

1. Enter system view.
system-view
 2. Enable MKA session logging.
macsec mka-session log enable
- By default, MKA session logging is disabled.

Display and maintenance commands for MACsec

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display MACsec information on ports.	display macsec [interface <i>interface-type interface-number</i>] [verbose]
Display MKA policy information.	display mka { default-policy policy [name <i>policy-name</i>] }
Display MKA session information.	display mka session [interface <i>interface-type interface-number</i> local-sci <i>sci-id</i>] [verbose]
Display MKA statistics on ports.	display mka statistics [interface <i>interface-type interface-number</i>]
Reset MKA sessions on ports.	reset mka session [interface <i>interface-type interface-number</i>]
Clear MKA statistics on ports.	reset mka statistics [interface <i>interface-type interface-number</i>]

Troubleshooting MACsec

Cannot establish MKA sessions between MACsec devices

Symptom

The devices cannot establish MKA sessions when the following conditions exist:

- The link connecting the devices is up.
- The ports at the ends of the link are MACsec capable.

Analysis

The symptom might occur for the following reasons:

- The ports at the link are not enabled with MKA.
- A port at the link is not configured with a preshared key or configured with a preshared key different from the peer.

Solution

To resolve the issue:

1. Enter interface view.
2. Use the **display this** command to check the MACsec configuration:
 - If MKA is not enabled on the port, execute the **mka enable** command.
 - If a preshared key is not configured or the preshared key is different from the peer, use the **mka psk** command to configure a preshared key. Make sure the preshared key is the same as the preshared key on the peer.
3. If the issue persists, contact H3C Support.

Command reference

confidentiality-offset

Use **confidentiality-offset** to set the MACsec confidentiality offset in an MKA policy.

Use **undo confidentiality-offset** to restore the default.

Syntax

confidentiality-offset *offset-value*

undo confidentiality-offset

Default

The MACsec confidentiality offset is 0. The entire frame is encrypted.

Views

MKA policy view

Predefined user roles

network-admin

Parameters

offset-value: Specifies the confidentiality offset in bytes. The value can be 0, 30 or 50.

Usage guidelines

The MACsec confidentiality offset specifies the number of bytes starting from the frame header. MACsec encrypts only the bytes after the offset in a frame.

When an MKA policy is applied to a port, the MACsec confidentiality offset in the policy overwrites the confidentiality offset previously configured on the port. However, MACsec uses the confidentiality offset propagated by the key server.

Examples

```
# Set the MACsec confidentiality offset to 30 bytes in MKA policy abcd.
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd] confidentiality-offset 30
```

Related commands

macsec confidentiality-offset

mka apply policy

display macsec

Use **display macsec** to display MACsec information on ports.

Syntax

```
display macsec [ interface interface-type interface-number ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MACsec information on all ports.

verbose: Displays detailed MACsec information. If you do not specify this keyword, the command displays brief MACsec information.

Examples

```
# Display brief MACsec information on GigabitEthernet 1/0/1.
```

```
<Sysname> display macsec interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
  Protect frames           : Yes
  Active MKA policy       : PL01
  Replay protection       : Enabled
  Replay window size      : 0 frames
  Confidentiality offset  : 0 bytes
  Validation mode         : Check
```

```
# Display detailed MACsec information on GigabitEthernet 1/0/1.
```

```
<Sysname> display macsec interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
  Protect frames           : Yes
```



```

Active MKA policy      : PL01
Replay protection      : Enabled
Replay window size    : 0 frames
Confidentiality offset : 0 bytes
Validation mode        : Check
Included SCI           : No
SCI conflict           : No
Cipher suite           : GCM-AES-128
Transmit secure channel:
  SCI                  : 000C29F6A4380004
  Elapsed time: 00h:02m:19s
  Current SA   : AN 0          PN 1
Receive secure channels:
  SCI          : 000C29258D430124
  Elapsed time: 00h:02m:17s
  Current SA   : AN 0          LPN 1
  Previous SA  : AN N/A       LPN N/A

```

Table 96 Command output

Field	Description
Protect frames	Status of MACsec desire on the port: • Yes. • No. If the port does not have an MKA principal actor, this field displays N/A.
Active MKA policy	MKA policy applied to the port. This field displays N/A if the port is not enabled with MACsec desire. This field is not available if the port is enabled with MACsec desire but is not applied an MKA policy.
Replay protection	Status of replay protection on the port: • Enabled. • Disabled. If the port is not enabled with MACsec desire, this field displays N/A.
Replay window size	Replay protection window size in number of frames. This field displays N/A in the following situations: • The port is not enabled with MACsec desire. • The port is not enabled with replay protection.
Confidentiality offset	Confidentiality offset in bytes. If the port is not enabled with MACsec desire, this field displays N/A.
Validation mode	Validation mode: • Check. • Disabled. • Strict. If the port is not enabled with MACsec desire, this field displays N/A.
Included SCI	Whether the frame includes SCI tag: • Yes. • No. If the port is not enabled with MACsec desire, this field displays N/A.

Field	Description
SCI conflict	Whether the SCI in the received MKA packets is the same as the local SCI: Yes—The SCI in the received MKA packets is the same as the local SCI. No—No MKA packet is received, or the SCI in the received MKA packets is different from the local SCI.
Cipher suite	Cipher suite for MACsec encryption: - GCM-AES-128. - GCM-AES-256. If the port is not enabled with MACsec desire, this field displays N/A .
Transmit secure channel	Information about the secure channel for outbound traffic. This field is not available if the port is not enabled with MACsec desire.
Receive secure channel	Information about the secure channel for inbound traffic. This field is not available if the port is not enabled with MACsec desire.
Elapsed time	Lifetime of the secure channel.
SCI	A hexadecimal string that contains the MAC address and port ID.
Current SA	Current SA used by the secure channel. If no current SA is available, each of the AN, PN, and LPN fields for the current SA displays N/A .
Previous SA	Previous SA used by the secure channel. If no previous SA is available, each of the AN and LPN fields for the previous SA displays N/A .
PN	Packet number for outbound traffic.
AN	SA number.
LPN	The minimum received packet number allowed by SAK.

Related commands

mka apply policy

display mka policy

Use **display mka policy** to display MKA policy information.

Syntax

display mka { **default-policy** | **policy** [**name** *policy-name*] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

default-policy: Specifies the system-defined MKA policy.

policy: Specifies an MKA policy or all MKA policies.

name *policy-name*: Specifies an MKA policy by policy name. The *policy-name* argument represents the MKA policy name, a case-sensitive string of 1 to 16 characters. If you do not specify an MKA policy, this command displays information about all MKA policies.

Examples

Display information about all MKA policies.

```
<Sysname> display mka policy
```

PolicyName	ReplayProtection	WindowSize	ConfOffset	Validation
default-policy	Yes	0	0	Check
policy1	Yes	0	30	Check
policy2	Yes	100	0	Disabled
policy3	No	0	0	Strict
policy4	Yes	200	50	Check
policy5	Yes	0	0	Check

Table 97 Command output

Field	Description
PolicyName	Name of the MKA policy.
ReplayProtection	Whether the replay protection feature is enabled.
WindowSize	Replay protection window size in number of frames.
ConfOffset	Confidentiality offset in bytes.
Validation	Validation mode: • Check. • Disabled. • Strict.

Related commands

mka policy

mka apply policy

display mka session

Use **display mka session** to display MKA session information.

Syntax

```
display mka session [ interface interface-type interface-number | local-sci sci-id ]  
[ verbose ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MKA session information on all ports.

local-sci sci-id: Specifies a local SCI, a case-insensitive hexadecimal string of 16 characters.

verbose: Displays detailed MKA session information. If you do not specify this keyword, the command displays brief MKA session information.

Examples

Display brief MKA session information on GigabitEthernet 1/0/1.

```
<Sysname> display mka session interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
Tx-SCI      : 000C29F6A4380004
Priority     : 0
Capability: 3
  CKN for participant: ABCD
    Key server      : Yes
    MI (MN)         : D7B00EDA353242704CC6B0DB (7)
    Live peers      : 1
    Potential peers  : 0
    Principal actor  : Yes
    MKA session status : Secured
    Confidentiality offset: 30 bytes
```

Display detailed MKA session information on GigabitEthernet 1/0/1.

```
<Sysname> display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI      : 000C29F6A4380004
Priority     : 0
Capability: 3
  CKN for participant: ABCD
    Key server      : Yes
    MI (MN)         : D7B00EDA353242704CC6B0DB (7)
    Live peers      : 1
    Potential peers  : 0
    Principal actor  : Yes
    MKA session status : Secured
    Confidentiality offset: 30 bytes
    Current SAK status : Rx & Tx
    Current SAK AN     : 0
    Current SAK KI (KN) : 4273791304C1C26259C94C3400000001 (1)
    Previous SAK status : N/A
    Previous SAK AN     : N/A
    Previous SAK KI (KN) : N/A
    Live peer list:
      MI              MN              Priority  Capability  Rx-SCI
      EA58DC3F8715953DBC6593F0  840      100        3          00E0020000000106

    Potential peer list:
      MI              MN              Priority  Capability  Rx-SCI
      DA58DC3Q4573543DBC6699F0  3        200        3          00E0021200000107
```

Table 98 Command output

Field	Description
Tx-SCI	SCI for outbound traffic, in hexadecimal notation.
Priority	Key server priority, in the range of 0 to 255.
Capability	MACsec capability: • 0—The port is MACsec incapable. • 1—The port supports integrity check only. • 2—The port supports integrity check and packet encryption. The confidentiality offset must be 0. • 3—The port supports integrity check and packet encryption. The confidentiality offset can be 0, 30, or 50.
CKN for participant	CAK name of the MKA instance.
Key server	Whether the local end is the key server.
MI	Member identifier in hexadecimal notation.
MN	Message number.
Live peers	Numbers of peers that have already been learned.
Potential peers	Numbers of peers that are being negotiated.
Principal actor	Whether the MKA instance is the principal actor. MKA instance refers to the operation entity of the MKA protocol on a port. A port might have multiple MKA instances. The principal actor is the MKA instance in active state.
MKA session status	MKA session status: • Unknown. • Pending. • Unauthenticated—The port has not been authenticated. • Authenticated—The port has passed the 802.1X authentication. • Secured—The session will be secured. If the MKA instance is not the principal actor, this field displays N/A.
Confidentiality offset	Confidentiality offset issued by the key server. This field displays N/A in the following situations: • The packet is transmitted in plain text. • The MKA instance is not the principal actor.
Current SAK status	Status of the current SAK: • Tx—The SAK is used to send packets. • Rx—The SAK is used to receive packets. This field displays N/A in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.
Current SAK AN	SA number of the current SAK in use. This field displays N/A in the following situations: • The MKA instance is not the principal actor. • The SAK does not exist.

Field	Description
Current SAK KI	Key identifier of the current SAK in use, a string of hexadecimal digits that contains the key server's 12-byte MI and KN. This field displays N/A in the following situations: - The MKA instance is not the principal actor. - The SAK does not exist.
KN	SAK number. This field displays N/A in the following situations: - The MKA instance is not the principal actor. - The SAK does not exist.
Previous SAK status	Status of the previous SAK: Tx—The SAK is used to send packets. Rx—The SAK is used to receive packets. This field displays N/A in the following situations: - The MKA instance is not the principal actor. - The SAK does not exist.
Previous SAK AN	SA number of the previous SAK. This field displays N/A in the following situations: - The MKA instance is not the principal actor. - The SAK does not exist.
Previous SAK KI	Key identifier of the previous SAK, a string of hexadecimal digits that contains the key server's 12-byte MI and KN. This field displays N/A in the following situations: - The MKA instance is not the principal actor. - The SAK does not exist.
Live peer list	List of peers that have participated in the MKA session. This field is not available if no live peer exists.
Potential peer list	List of peers that are being negotiated. This field is not available if no potential peer exists.
Rx-SCI	SCI for inbound traffic, in hexadecimal notation.

Related commands

reset mka session

display mka statistics

Use **display mka statistics** to display MKA statistics on ports.

Syntax

display mka statistics [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays MKA statistics on all ports.

Examples

Display MKA statistics on GigabitEthernet 1/0/1.

```
<Sysname> display mka statistics interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1 statistics
MKPDUs with invalid CKN : 0
MKPDUs with invalid ICV : 0
MKPDUs with Rx error    : 0
CKN for participant      : ABCD
    Tx MKPDUs           : 2379
    Rx MKPDUs           : 2375
MKPDUs with invalid MN : 0
MKPDUs with Tx error   : 0
SAKs distributed        : 0
SAKs received           : 5
```

Table 99 Command output

Field	Description
MKPDUs with invalid CKN	Number of received MKA packets with invalid CKNs.
MKPDUs with invalid ICV	Number of MKA packets that failed ICV check.
MKPDUs with Rx error	Number of received error MKA packets.
CKN for participant	CAK name of the MKA instance.
Tx MKPDUs	Number of the MKA packets sent by the MKA instance.
Rx MKPDUs	Number of the MKA packets received by the MKA instance.
MKPDUs with invalid MN	Number of MKA packets with illegal MNs received by the MKA instance.
MKPDUs with Tx error	Number of error MKA packets sent by the MKA instance.
SAKs distributed	Number of SAKs distributed by the MKA instance.
SAKs received	Number of SAKs received by the MKA instance.

Related commands

reset mka statistics

macsec cipher-suite

Use **macsec cipher-suite** to specify the cipher suite for MACsec encryption.

Use **undo macsec cipher-suite** to restore the default.

Syntax

macsec cipher-suite { **gcm-aes-128** | **gcm-aes-256** }

undo macsec cipher-suite

Default

MACsec uses the GCM-AES-128 cipher suite for encryption.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

gcm-aes-128: Specifies the GCM-AES-128 cipher suite.

gcm-aes-256: Specifies the GCM-AES-256 cipher suite.

Usage guidelines

Do not use this command on an 802.1X-enabled port.

This command is supported only in device-oriented mode. Make sure the connected ports are configured with the same cipher suite. If the ports are configured with different cipher suites, they cannot successfully establish MKA sessions.

Examples

Specify the GCM-AES-256 cipher suite for MACsec encryption on GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] macsec cipher-suite gcm-aes-256
```

Related commands

dot1x

mka psk

macsec confidentiality-offset

Use **macsec confidentiality-offset** to set the MACsec confidentiality offset on a port.

Use **undo macsec confidentiality-offset** to restore the default.

Syntax

macsec confidentiality-offset *offset-value*

undo macsec confidentiality-offset

Default

The MACsec confidentiality offset on the port is 0. The entire frame is encrypted.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

offset-value: Specifies the confidentiality offset in bytes. The value can be 0, 30 or 50.

Usage guidelines

The MACsec confidentiality offset specifies the number of bytes starting from the frame header. MACsec encrypts only the bytes after the offset in a frame.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the confidentiality offset in the MKA policy. The MKA policy application is removed from the port. However, other settings (settings for parameters except the confidentiality offset) of the MKA policy are effective on the port.

MACsec uses the MACsec confidentiality offset propagated by the key server.

Examples

```
# Set the MACsec confidentiality offset to 30 bytes on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec confidentiality-offset 30
```

Related commands

confidentiality-offset

display macsec

display mka session

mka apply policy

macsec desire

Use **macsec desire** to enable MACsec desire. The port expects MACsec protection for outbound frames.

Use **undo macsec desire** to disable MACsec desire.

Syntax

macsec desire

undo macsec desire

Default

MACsec desire is disabled. A port does not expect MACsec protection for outbound frames.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command allows a MACsec port to expect MACsec protection for outbound frames. The key server determines whether MACsec protects the outbound frames.

MACsec protects the outbound frames of the port when the following requirements are met:

- The key server is MACsec capable.
- Both the local participant and its peer are MACsec capable.
- A minimum of one participant is enabled with the MACsec desire feature.

Examples

```
# Enable MACsec desire on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec desire
```

macsec mka-session log enable

Use **macsec mka-session log enable** to enable MKA session logging.

Use **undo macsec mka-session log enable** to disable MKA session logging.

Syntax

macsec mka-session log enable

undo macsec mka-session log enable

Default

MKA session logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to generate logs for MKA session changes, such as peer aging and SAK updates. The logs are sent to the information center of the device. For the logs to be output correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable MKA session logging to prevent excessive log output.

Examples

```
# Enable MKA session logging.
<Sysname> system-view
[Sysname] macsec mka-session log enable
```

Related commands

info-center source (*Network Management and Monitoring Command Reference*)

macsec replay-protection enable

Use **macsec replay-protection enable** to enable MACsec replay protection on a port.

Use **undo macsec replay-protection enable** to disable MACsec replay protection on a port.

Syntax

macsec replay-protection enable

undo macsec replay-protection enable

Default

MACsec replay protection is enabled on the port.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This feature allows a MACsec port to accept a number of out-of-order or repeated inbound frames.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the MACsec replay protection configuration in the MKA policy. The MKA policy application is removed from the port. However, other settings (settings for parameters except MACsec replay protection) of the MKA policy are effective on the port.

Examples

```
# Enable MACsec replay protection on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec replay-protection enable
```

Related commands

display macsec
macsec replay-protection window-size
mka apply policy
replay-protection enable

macsec replay-protection window-size

Use **macsec replay-protection window-size** to set the MACsec replay protection window size on a port.

Use **undo macsec replay-protection window-size** to restore the default.

Syntax

macsec replay-protection window-size *size-value*
undo macsec replay-protection window-size

Default

The MACsec replay protection window size is 0 on a port. The device accepts only frames that arrive in the correct order. Out-of-order or duplicated frames will be dropped.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

size-value: Specifies the replay protection window size, in the range of 0 to 4294967295 frames.

Usage guidelines

To allow a MACsec port to accept a number of out-of-order frames, enable replay protection and specify a replay protection window size on the port.

Suppose the replay protection window size is **a** on a port. After the port receives a packet with packet number (PN) **x**, it can accept only packets whose PN is greater than or equal to **x-a**.

The replay protection window size takes effect only when the replay protection feature is enabled on the port.

Set a replay protection window size based on the forwarding path of frames. If the frames might be forwarded multiple times, set a large replay protection window size.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the replay protection window size in the MKA policy. The MKA policy application is

removed from the port. However, other settings (settings for parameters except the replay protection window size) of the MKA policy are effective on the port.

Examples

```
# Set the MACsec replay protection window size to 100 on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] macsec replay-protection window-size 100
```

Related commands

display macsec
macsec replay-protection enable
mka apply policy
replay-protection window-size

macsec validation mode

Use **macsec validation mode** to set a MACsec validation mode on a port.

Use **undo macsec validation mode** to restore the default.

Syntax

macsec validation mode { check | disabled | strict }
undo macsec validation mode

Default

The MACsec validation mode is **check** on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

check: Performs validation only and does not drop illegal frames.
disabled: Does not perform validation.
strict: Performs validation and drops illegal frames.

Usage guidelines

To avoid data loss, use the default validation mode **check** on the MACsec devices in case of MKA negotiation failure. After you use the **display macsec** command to verify that MKA negotiation has succeeded, change the validation mode to **strict**.

If you execute this command on a port to which an MKA policy has been applied, the configuration overwrites the validation mode in the MKA policy. The MKA policy application is removed from the port. However, other settings (settings for parameters except the validation mode) of the MKA policy are effective on the port.

Examples

```
# Set the MACsec validation mode to strict on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] macsec validation mode strict
```

Related commands

display macsec
mka apply policy
validation mode

mka apply policy

Use **mka apply policy** to apply an MKA policy to a port.

Use **undo mka apply policy** to remove the MKA policy from a port.

Syntax

mka apply policy *policy-name*
undo mka apply policy

Default

No MKA policy is applied to the port.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of an MKA policy, a case-sensitive string of 1 to 16 characters.

Usage guidelines

An MKA policy defines MACsec parameters, including confidentiality offset, validation mode, replay protection, and replay protection window size.

When you apply an MKA policy to a port, the MACsec parameter settings in the policy overwrite the MACsec parameters previously configured on the port. Any modifications to the MKA policy take effect immediately.

When you remove the MKA policy from a port, the MACsec parameter settings on the port restore to the default.

The MKA policy applied to a port is automatically removed from that port when you delete the policy. No MKA policy will run on that port until after you apply one to it.

When you apply a nonexistent MKA policy to a port, the port automatically uses the system-defined MKA policy **default-policy**. After you create the specified policy, the policy will be automatically applied to the port.

Examples

Apply MKA policy **abcd** to GigabitEthernet 1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mka apply policy abcd
```

Related commands

confidentiality-offset
display mka policy

replay-protection enable
replay-protection window-size
validation mode

mka enable

Use **mka enable** to enable MKA on a port.
Use **undo mka enable** to disable MKA on a port.

Syntax

mka enable
undo mka enable

Default

MKA is disabled on a port.

Views

Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

MKA establishes and manages MACsec secure channels on a port. It also negotiates encryption keys used by MACsec.

The enabling of MKA on a port triggers MKA negotiation. After MKA negotiation succeeds, an MKA session is successfully established.

Examples

```
# Enable MKA on GigabitEthernet 1/0/1.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mka enable
```

Related commands

display mka session

mka policy

Use **mka policy** to create an MKA policy and enter its view, or enter the view of an existing MKA policy.

Use **undo mka policy** to delete an MKA policy.

Syntax

mka policy *policy-name*
undo mka policy *policy-name*

Default

A system-defined MKA policy exists. The policy name is default-policy.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies the name of an MKA policy, a case-sensitive string of 1 to 16 characters.

Usage guidelines

MKA policy provides a centralized method for configuring MACsec confidentiality offset, validation mode, replay protection, and replay protection window size.

The system supports multiple MKA policies.

You cannot delete or modify the system-defined MKA policy **default-policy**.

Examples

Create an MKA policy named **abcd** and enter its view.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd]
```

Related commands

confidentiality-offset

display mka policy

mka apply policy

replay-protection enable

replay-protection window-size

validation mode

mka priority

Use **mka priority** to set the MKA key server priority.

Use **undo mka priority** to restore the default.

Syntax

mka priority *priority-value*

undo mka priority

Default

The MKA key server priority is 0.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Specifies the priority value, in the range of 0 to 255. The priority is inversely related to its value.

Usage guidelines

If you use 802.1X-generated CAK, the access device port automatically becomes the key server.

The port that has higher priority (lower priority value) becomes the key server if you use a preshared key as the CAK. If the port and its peers have the same priority, MACsec compares the SCI values on the ports. The port with the lowest SCI value becomes the key server.

A port with priority 255 cannot become the key server. For a successful key server selection, make sure a minimum of one participant's key server priority is not 255.

Examples

```
# Set the MKA key server priority to 2 on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mka priority 2
```

Related commands

display mka session

mka psk

Use **mka psk** to set a preshared key as the CAK.

Use **undo mka psk** to restore the default.

Syntax

mka psk ckn *name* **cak** { **cipher** | **simple** } *string*

undo mka psk

Default

No preshared key exists.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

ckn *name*: Specifies the preshared key name, a hexadecimal string with an even number of case-insensitive characters. The name length is in the range of 2 to 64 characters.

cak: Specifies the preshared key.

cipher: Specifies the preshared key in encrypted form.

simple: Specifies the preshared key in plaintext form. For security purposes, the preshared key specified in plaintext form will be stored in encrypted form.

string: Specifies the preshared key. Its plaintext form is an even number of case-insensitive hexadecimal digits in the range of 2 to 64 characters. Its encrypted form is a case-sensitive string of 2 to 117 characters.

Usage guidelines

The CAK can be either generated during 802.1X or manually configured at the CLI. The manually configured CAK takes precedence over the 802.1X-generated key.

When 802.1X is not enabled on MACsec ports, you can execute this command to configure a preshared key on each MACsec port. Make sure the connected MACsec ports are configured with

the same CAK and CKN. If the connected ports are configured with different CAKs or CKNs, they cannot successfully establish MKA sessions.

To successfully establish an MKA session between two connected ports, make sure only the ports are configured with the same CKN in the network.

To delete the configured keys for MKA sessions that have been established, perform the following tasks:

1. Execute the **undo mka psk** command on the key server.
2. Execute the **undo mka psk** command on the non-key server.

The deletion operation deletes the established MKA sessions at the same time.

Different cipher suites for MACsec encryption have different requirements for the CKN and CAK configuration.

- The GCM-AES-128 cipher suite requires that the CKN and CAK each must be 32 characters long. If the configured CKN or CAK is not 32 characters long, the system performs the following operations when it runs the cipher suite:
 - Automatically increases the length of the CKN or CAK by zero padding if the CKN or CAK contains less than 32 characters.
 - Uses only the first 32 characters if the CKN or CAK contains more than 32 characters.
- The GCM-AES-256 cipher suite requires that the CKN and CAK each must be 64 characters long. If the configured CKN or CAK contains less than 64 characters, the system automatically increases the length of the CKN or CAK by zero padding when it runs the cipher suite.

Examples

```
# Configure the CAK name as AB, and set the CAK to 1234 in plain text on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mka psk ckn AB cak simple 1234
```

Related commands

dot1x

macsec cipher-suite

mka timer mka-life

Use **mka timer mka-life** to set the MKA life time.

Use **undo mka timer mka-life** to restore the default.

Syntax

mka timer mka-life *seconds*

undo mka timer mka-life

Default

The MKA life time is 6 seconds.

Views

Ethernet interface view

Predefined user roles

network-admin

mdc-admin

Parameters

seconds: Sets the MKA life time in seconds. The value range for this argument is 6 to 600.

Usage guidelines

The participants at each end of a secure session exchange MKA protocol packets to keep the session alive.

The MKA life time sets the session keepalive timer for participants. The timer starts on a participant when the participant receives the first MKA protocol packet from its peer. If the participant does not receive any subsequent MKA protocol packets from that peer before the timer expires, the participant determines that the session is insecure and then removes the session.

This command is applicable only in device-oriented mode.

Make sure the participants at each end of a secure session have the same MKA life time.

Examples

Set the MKA life time to 10 seconds on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mka timer mka-life 10
```

Related commands

display macsec

replay-protection enable

Use **replay-protection enable** to enable MACsec replay protection in an MKA policy.

Use **undo replay-protection enable** to disable MACsec replay protection in an MKA policy.

Syntax

replay-protection enable

undo replay-protection enable

Default

MACsec replay protection is enabled in an MKA policy.

Views

MKA policy view

Predefined user roles

network-admin

Usage guidelines

This feature allows a MACsec port to accept a number of out-of-order or repeated inbound frames.

When an MKA policy is applied to a port, the replay protection configuration in the policy overwrites the replay protection feature already used by the port.

Examples

Enable MACsec replay protection in MKA policy **abcd**.

```
<Sysname> system-view
[Sysname] mka policy abcd
[Sysname-mka-policy-abcd] replay-protection enable
```

Related commands

macsec replay-protection enable

mka apply policy

replay-protection window-size

replay-protection window-size

Use **replay-protection window-size** to set the MACsec replay protection window size in an MKA policy.

Use **undo replay-protection window-size** to restore the default.

Syntax

replay-protection window-size *size-value*

undo replay-protection window-size

Default

The MACsec replay protection window size in an MKA policy is 0. The device accepts only frames that arrive in the correct order. Out-of-order or duplicated frames will be dropped.

Views

MKA policy view

Predefined user roles

network-admin

Parameters

size-value: Specifies the replay protection window size, in the range of 0 to 4294967295 frames.

Usage guidelines

The MACsec replay protection window size allows a MACsec port to accept a number of out-of-order inbound frames.

Suppose the replay protection window size is **a** on a port. After the port receives a packet with PN **x**, it can accept only packets whose PN is greater than or equal to **x-a**.

The replay protection window size takes effect only when the replay protection feature is enabled on the port.

Set a replay protection window size based on the forwarding path of frames. If the frames might be forwarded multiple times, set a large replay protection window size.

When an MKA policy is applied to a port, the replay protection window size in the policy overwrites the window size already configured on the port.

Examples

Set the MACsec replay protection window size to 100 in MKA policy **abcd**.

```
<Sysname> system-view
```

```
[Sysname] mka policy abcd
```

```
[Sysname-mka-policy-abcd] replay-protection window-size 100
```

Related commands

macsec replay-protection window-size

macsec replay-protection enable

mka apply policy

reset mka session

Use **reset mka session** to reset MKA sessions on ports.

Syntax

reset mka session [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command resets MKA sessions on all ports.

Usage guidelines

This command first clears MKA sessions, and then immediately triggers a new session establishment negotiation.

Examples

```
# Reset MKA sessions on GigabitEthernet 1/0/1.  
<Sysname> reset mka session interface gigabitethernet 1/0/1
```

Related commands

display mka session

reset mka statistics

Use **reset mka statistics** to clear MKA statistics on ports.

Syntax

reset mka statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command clears MKA statistics on all ports.

Examples

```
# Clear MKA statistics on GigabitEthernet 1/0/1.  
<Sysname> reset mka statistics interface gigabitethernet 1/0/1
```

Related commands

display mka statistics

validation mode

Use **validation mode** to set a MACsec validation mode in an MKA policy.

Use **undo validation mode** to restore the default.

Syntax

validation mode { **check** | **disabled** | **strict** }

undo validation mode

Default

The MACsec validation mode is **check**. The device performs validation only and does not drop illegal frames.

Views

MKA policy view

Predefined user roles

network-admin

Parameters

check: Performs validation only and does not drop illegal frames.

disabled: Does not perform validation.

strict: Performs validation and drops illegal frames.

Usage guidelines

To avoid data loss, use the default validation mode **check** on the MACsec devices in case of MKA negotiation failure. After you use the **display macsec** command to verify that MKA negotiation has succeeded, change the validation mode to **strict**.

When an MKA policy is applied to a port, the MACsec validation mode in the policy overwrites the MACsec validation mode already configured on the port.

Examples

Set the MACsec validation mode to **strict** in MKA policy **abcd**.

```
<Sysname> system-view
```

```
[Sysname] mka policy abcd
```

```
[Sysname-mka-policy-abcd] validation mode strict
```

Related commands

macsec validation mode

mka apply policy

New feature: Configuring the device as responder-only for IPsec SA negotiation

Configuring the device as responder-only for IPsec SA negotiation

About this task

By default, two IPsec peers will both initiate the establishment of an IPsec SA when they both use an IKE-based IPsec profile to established IPsec SAs. In this case, the two IPsec peers use two IPsec negotiation processes to establish one IPsec SA, wasting CPU resources.

To resolve this issue, you can enable the responder-only mode. After you configure a device as a responder-only device, the device will not initiate IPsec SAs but respond to negotiations initiated by its peers.

Restrictions and guidelines

As a best practice, configure this feature on the hub device in a hub-spoke network.

Procedure

1. Enter system view.

system-view

2. Enter IPsec policy view, IPsec policy template view, or IPsec profile view.

- o Enter IPsec policy view.

- **ipsec { ipv6-policy | policy } policy-name seq-number isakmp**

- o Enter IPsec policy template view

- **ipsec { ipv6-policy-template | policy-template } template-name seq-number**

- o Enter IPsec profile view.

- **ipsec profile profile-name isakmp**

3. Enable the responder-only mode for IPsec SA negotiation.

responder-only enable

By default, the responder-only mode is disabled.

Command reference

New command: responder-only enable

Use **responder-only enable** to enable the responder-only mode.

Use **undo responder-only enable** to disable the responder-only mode.

Syntax

responder-only enable

undo responder-only enable

Default

The responder-only mode of the device is disabled.

Views

- IPsec profile view
- IPsec policy view
- IPsec policy template view

Predefined user roles

- network-admin

Usage guidelines

As a best practice, configure this feature on the hub device in a hub-spoke network.

By default, two IPsec peers will both initiate the establishment of an IPsec SA when they both use an IKE-based IPsec profile to establish IPsec SAs. In this case, the two IPsec peers use two IPsec negotiation processes to establish one IPsec SA, wasting CPU resources. To resolve this issue, you can enable the responder-only mode. After you configure a device as a responder-only device, the device will not initiate IPsec SAs but respond to negotiations initiated by its peers.

Enabling or disabling this command does not affect existing IPsec SAs.

Examples

In IPsec profile **prof1**, configure the device as responder-only for IPsec SA negotiation.

```
<Sysname> system-view
[Sysname] ipsec profile prof1 isakmp
[Sysname-ipsec-profile-prof1] responder-only enable
```

In IPsec policy **map**, configure the device as responder-only for IPsec SA negotiation.

```
<Sysname> system-view
[Sysname] ipsec policy map 1 isakmp
[Sysname-ipsec-policy-isakmp-map-1] responder-only enable
```

Related commands

- display ipsec { ipv6-policy | policy }**
- display ipsec { ipv6-policy-template | policy-template }**
- display ipsec profile**

Modified command: **display ipsec { ipv6-policy | policy }**

Syntax

display ipsec { ipv6-policy | policy } [*policy-name* [*seq-number*]]

Views

- Any view

Change description

The **Responder only** field is added to the output for this command.

```
<Sysname> display ipsec policy
-----
IPsec Policy: mypolicy
-----

-----
Sequence number: 1
```

```

Alias: mypolicy-1
Mode: Manual
-----
The policy configuration is incomplete:
    ACL not specified
    Incomplete transform-set configuration
Description: This is my first IPv4 manual policy
Security data flow:
Remote address: 2.5.2.1
Transform set: transform

Inbound AH setting:
    AH SPI: 1200 (0x000004b0)
    AH string-key: *****
    AH authentication hex key:

Inbound ESP setting:
    ESP SPI: 1400 (0x00000578)
    ESP string-key:
    ESP encryption hex key:
    ESP authentication hex key:

Outbound AH setting:
    AH SPI: 1300 (0x00000514)
    AH string-key: *****
    AH authentication hex key:

Outbound ESP setting:
    ESP SPI: 1500 (0x000005dc)
    ESP string-key: *****
    ESP encryption hex key:
    ESP authentication hex key:

-----
Sequence number: 2
Alias: mypolicy-2
Mode: ISAKMP
-----
The policy configuration is incomplete:
    Remote-address not set
    ACL not specified
    Transform-set not set
Description: This is my first IPv4 Isakmp policy
Traffic Flow Confidentiality: Enabled
Security data flow:
Selector mode: standard
Local address:
Remote address: 5.2.2.1, primary, track 1 (track state: Positive)

```



```

Remote address: test, track 2 (track state: Positive)
Remote address switchback mode: Enabled
Transform set:
IKE profile:
IKEv2 profile:
smart-link policy:
SA trigger mode: Auto
SA duration(time based): 3600 seconds
SA duration(traffic based): 1843200 kilobytes
SA soft-duration buffer(time based): 1000 seconds
SA soft-duration buffer(traffic based): 43200 kilobytes
SA idle time: 100 seconds
Responder only: Disabled

```

Table 100 Command output

Field	Description
Responder only	State of the responder only feature: • Enabled • Disabled

Modified command: display ipsec { ipv6-policy-template | policy-template }

Syntax

```

display ipsec { ipv6-policy-template | policy-template } [ template-name
[ seq-number ] ]

```

Views

Any view

Change description

The **Responder only** field is added to the output for this command.

```
<Sysname> display ipsec policy-template
```

```

-----
IPsec Policy Template: template
-----

```

```

-----
Sequence number: 1
Alias: template-template-1
-----

```

```

Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:

```

```

Remote address: 162.105.10.2
Transform set:  testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time: 100 seconds
Responder only: Disabled

```

Table 101 Command output

Field	Description
Responder only	State of the responder only feature: • Enabled • Disabled

Modified command: display ipsec profile

Syntax

display ipsec profile [*profile-name*]

Views

Any view

Change description

The **Responder only** field is added to the output for this command.

```

<Sysname> display ipsec profile
-----
IPsec profile: myprofile
Alias: ccc
Mode: isakmp
-----

Transform set:  tran1
IKE profile: profile
SA duration(time based): 3600 seconds
SA duration(traffic based): 1843200 kilobytes
SA soft-duration buffer(time based): 1000 seconds
SA soft-duration buffer(traffic based): 43200 kilobytes
SA idle time: 100 seconds
Responder only: Disabled

```

Table 102 Command output

Field	Description
Responder only	State of the responder only feature: • Enabled • Disabled

Modified command: display ipsec statistics

Syntax

display ipsec statistics [**tunnel-id** *tunnel-id*]

Views

Any view

Change description

The **Responder only limitation** field is added to the output for this command.

```
<Sysname> display ipsec statistics
IPsec packet statistics:
  Received/sent packets: 47/64
  Received/sent bytes: 3948/5208
  Received/sent packet rate: 5/5 packets/sec
  Received/sent byte rate: 290/290 bytes/sec
  Dropped packets (received/sent): 0/45

Dropped packets statistics
  No available SA: 0
  Wrong SA: 0
  Invalid length: 0
  Authentication failure: 0
  Encapsulation failure: 0
  Decapsulation failure: 0
  Replayed packets: 0
  ACL check failure: 45
  MTU check failure: 0
  Loopback limit exceeded: 0
  Crypto speed limit exceeded: 0
  Responder only limitation: 0
```

Table 103 Command output

Field	Description
Responder only limitation	Number of packets dropped due to responder only limitation.

New feature: Specifying a security enhanced level

Specifying a security enhanced level

About this task

The security enhanced level for the device can be 1 and 2, and level 2 indicates a higher security level. If the security enhanced level is set to 2, the following rules apply:

- SSL client policies and SSL server policies do not support cipher suites that contain DES, 3DES, MD5, RC4, and RC2.

- SSL client policies and SSL server policies do not support SSL protocol versions lower than TLS 1.1.
- SSL session renegotiation cannot be enabled.

You can specify a security enhanced level as needed.

Restrictions and guidelines

After you change the security enhanced level, for services associated with SSL policies, such as HTTP and SSL VPN, you must re-enable these services to update the associated policies.

Procedure

1. Enter system view.
system-view
2. Specify a security enhanced level for the device.
security-enhanced level *level-value*

The default setting varies by device model. For more information, see the command reference.

Command reference

security-enhanced level

Use **security-enhanced level** to specify a security enhanced level for the device.

Use **undo security-enhanced level** to restore the default.

Syntax

security-enhanced level *level-value*

undo security-enhanced level

Default

Hardware	Default
MSR610	The security enhanced level is 2 for the device.
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	The security enhanced level is 1 for the device.
MSR810-LMS, MSR810-LUS	The security enhanced level is 1 for the device.
MSR810-SI, MSR810-LM-SI	The security enhanced level is 1 for the device.
MSR810-LMS-EA, MSR810-LME	The security enhanced level is 1 for the device.
MSR1004S-5G, MSR1004S-5G-CN	The security enhanced level is 1 for the device.
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	The security enhanced level is 2 for the device.
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	The security enhanced level is 1 for the device.
MSR2600-10-X1	The security enhanced level is 1 for the device.

Hardware	Default
MSR2630	The security enhanced level is 1 for the device.
MSR3600-28, MSR3600-51	The security enhanced level is 1 for the device.
MSR3600-28-SI, MSR3600-51-SI	The security enhanced level is 1 for the device.
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	The security enhanced level is 1 for the device.
MSR3600-28-G-DP, MSR3600-51-G-DP	The security enhanced level is 2 for the device.
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	The security enhanced level is 1 for the device.
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	The security enhanced level is 2 for the device.
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	The security enhanced level is 1 for the device.
MSR3610-G, MSR3620-G	The security enhanced level is 1 for the device.
MSR3640-G	The security enhanced level is 2 for the device.
MSR3640-X1-HI	The security enhanced level is 2 for the device.

Hardware	Default
MSR810-W-WiNet, MSR810-LM-WiNet	The security enhanced level is 1 for the device.
MSR830-4LM-WiNet	The security enhanced level is 1 for the device.
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	The security enhanced level is 1 for the device.
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	The security enhanced level is 1 for the device.
MSR2600-6-WiNet	The security enhanced level is 1 for the device.
MSR2600-10-X1-WiNet	The security enhanced level is 1 for the device.
MSR2630-WiNet	The security enhanced level is 1 for the device.
MSR3600-28-WiNet	The security enhanced level is 1 for the device.
MSR3610-X1-WiNet	The security enhanced level is 2 for the device.
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	The security enhanced level is 1 for the device.

Hardware	Default
MSR860-6EI-XS	The security enhanced level is 1 for the device.
MSR860-6HI-XS	The security enhanced level is 1 for the device.
MSR2630-XS	The security enhanced level is 1 for the device.
MSR3600-28-XS	The security enhanced level is 1 for the device.
MSR3610-XS	The security enhanced level is 2 for the device.
MSR3620-XS	The security enhanced level is 1 for the device.
MSR3610-I-XS	The security enhanced level is 1 for the device.
MSR3610-IE-XS	The security enhanced level is 1 for the device.
MSR3620-X1-XS	The security enhanced level is 2 for the device.
MSR3640-XS	The security enhanced level is 2 for the device.
MSR3660-XS	The security enhanced level is 2 for the device.

Hardware	Default
MSR810-LM-GL	The security enhanced level is 1 for the device.
MSR810-W-LM-GL	The security enhanced level is 1 for the device.
MSR830-6EI-GL	The security enhanced level is 1 for the device.
MSR830-10EI-GL	The security enhanced level is 1 for the device.
MSR830-6HI-GL	The security enhanced level is 1 for the device.
MSR830-10HI-GL	The security enhanced level is 1 for the device.
MSR1004S-5G-GL	The security enhanced level is 1 for the device.
MSR2600-6-X1-GL	The security enhanced level is 1 for the device.
MSR3600-28-SI-GL	The security enhanced level is 1 for the device.

Views

System view

Predefined user roles

network-admin

Parameters

level-value: Specifies the security enhanced level, which can be 1 and 2.

Usage guidelines

The security enhanced level for the device can be 1 and 2, and level 2 indicates a higher security level. If the security enhanced level is set to 2, the following rules apply:

- SSL client policies and SSL server policies do not support cipher suites that contain DES, 3DES, MD5, RC4, and RC2.
- SSL client policies and SSL server policies do not support SSL protocol versions lower than TLS 1.1.
- SSL session renegotiation cannot be enabled.

You can specify a security enhanced level as needed.

After you change the security enhanced level, for services associated with SSL policies, such as HTTP and SSL VPN, you must re-enable these services to update the associated policies.

Examples

Set the security enhanced level to 2 for the device.

```
<Sysname> system-view
```

```
[Sysname] security-enhanced level 2
```

New feature: Configuring GD-quantum encryption

Configuring GD-quantum encryption

About this task

After enabling GD-quantum encryption for IKE, the device can use the symmetric key provided by the GD-quantum server to encrypt the IPsec protected data, which further enhance the security of IPsec.

The device obtains keys from the GD-quantum server in the following steps:

1. **Connecting the GD-quantum server**—After all commands in IKE GD-quantum view are configured, the device establishes a connection with the specified GD-quantum server.
2. **Logging in to the GD-quantum server**—After the connection is established, the device sends a login request to the GD-quantum server, carrying the GD-quantum access ID and the GD-quantum authentication key. Only devices with verified GD-quantum access IDs and GD-quantum authentication keys can successfully log in to the GD-quantum server.
3. **Obtaining the GD-quantum keys**—After successful login and the IKE phase 1 negotiation, the device obtains the encrypted GD-quantum keys from the GD-quantum server, decrypt them with the GD-quantum decryption keys configured on the device, and finally obtain the GD-quantum keys for IPsec.

When enabling GD-quantum encryption for IKE, the device enters IKE GD-quantum view. Configure the IP address and port number of the GD-quantum server, the GD-quantum access IDs and GD-quantum authentication keys, and the GD-quantum decryption keys in this view.

Hardware and feature compatibility

Hardware	Feature compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes

Hardware	Feature compatibility
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Feature compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Feature compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Prerequisites

Before configuring the GD-quantum encryption feature, contact the administrator of the GD-quantum server to obtain the GD-quantum access ID, the GD-quantum authentication key, and the GD-quantum decryption key.

Procedure

1. Enter system view.
system-view
2. Enable GD-quantum encryption for IKE and enter IKE GD-quantum view.
ike gd-quantum
By default, GD-quantum encryption for IKE is disabled.
3. Specify the IP address and port number of the GD-quantum server.
server-address ip-address [port port-number]
By default, no IP address or port number of the GD-quantum server is specified.

4. Specify a GD-quantum access ID.
app-dev-info *app-dev-info*
 By default, no GD-quantum access ID is specified.
5. Configure a GD-quantum authentication key.
auth-key { **cipher** | **simple** } *key-value*
 By default, no GD-quantum authentication key is configured.
6. Configure a GD-quantum decryption key.
decrypt-quantum-key { **cipher** | **simple** } *key-value*
 By default, no GD-quantum decryption key is configured.

Command reference

app-dev-info (IKE GDQUANTUM view)

Use **app-dev-info** to specify a GD-quantum access ID.

Use **undo app-dev-info** to restore the default.

Syntax

app-dev-info *app-dev-info*

undo app-dev-info

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG,	No

Hardware	Command compatibility
MSR3610-IE-IG	
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No

Hardware	Command compatibility
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

No GD-quantum access ID is specified.

Views

IKE GD-quantum view

Predefined user roles

network-admin

Parameters

Yesapp-dev-info: Specifies a GD-quantum access ID, a nine-digit string.

Usage guidelines

The GD-quantum access IDs are uniformly distributed by the GD-quantum server, unique one for each device. You can use a GD-quantum access ID and a GD-quantum authentication key to log in to the GD-quantum server.

To obtain a GD-quantum access ID, contact the administrator of the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the GD-quantum access ID **185110851**.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum] app-dev-info 185110851
```

auth-key

Use **auth-key** to configure a GD-quantum authentication key.

Use **undo auth-key** to restore the default.

Syntax

auth-key { **cipher** | **simple** } *key-value*

undo auth-key

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No

Hardware	Command compatibility
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No

Hardware	Command compatibility
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

No GD-quantum authentication key is configured.

Views

IKE GD-quantum view

Predefined user roles

network-admin

Parameters

cipher: Specifies a GD-quantum authentication key in encrypted form.

simple: Specifies a GD-quantum authentication key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

key-value: Specifies the GD-quantum authentication key. The key is case sensitive. Its plaintext form is a 64-bit hexadecimal number, and its encrypted form is a 117-bit hexadecimal number.

Usage guidelines

The GD-quantum authentication keys are used by the GD-quantum server for identity authentication. Each GD-quantum authentication key corresponds to one GD-quantum access ID (specified by using the **app-dev-info** command). Only devices with correct GD-quantum access IDs and GD-quantum authentication keys can successfully log in to the GD-quantum server when sending login requests to the server.

To obtain a GD-quantum authentication key, contact the administrator of the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the GD-quantum authentication key
0x66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0 for logging in to
the GD-quantum server.

```
<Sysname> system-view
```

```
[Sysname] ike gd-quantum
```

```
[Sysname-ike-gdquantum] auth-key simple
```

```
66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0
```

decrypt-quantum-key

Use **decrypt-quantum-key** to configure a GD-quantum decryption key.

Use **undo decrypt-quantum-key** to restore the default.

Syntax

decrypt-quantum-key { **cipher** | **simple** } *key-value*

undo decrypt-quantum-key

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes

Hardware	Command compatibility
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No

Hardware	Command compatibility
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

No GD-quantum decryption key is configured.

Views

IKE GD-quantum view

Predefined user roles

network-admin

Parameters

cipher: Specifies a GD-quantum decryption key in encrypted form.

simple: Specifies a GD-quantum decryption key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

key-value: Specifies the GD-quantum decryption key. The key is case sensitive. Its plaintext form is a 64-bit hexadecimal number, and its encrypted form is a 117-bit hexadecimal number.

Usage guidelines

A device can request encrypted GD-quantum keys from the GD-quantum server after successfully logging in to the server. Use this command to configure GD-quantum decryption keys for decryption so as to be used in IPsec.

To obtain a GD-quantum decryption key, contact the administrator of the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
#          Configure          the          GD-quantum          decryption          key
0x66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0.

<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum] decrypt-quantum-key simple
66c7f0f462eedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0
```

ike gd-quantum

Use **ike gd-quantum** to enable GD-quantum encryption for IKE and enter IKE GD-quantum view.

Use **undo ike gd-quantum** to disable GD-quantum encryption for IKE.

Syntax

ike gd-quantum

undo ike gd-quantum

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No

Hardware	Command compatibility
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

GD-quantum encryption for IKE is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After enabling GD-quantum encryption for IKE, the device can use the symmetric key provided by the GD-quantum server to encrypt the IPsec protected data, which further enhance the security of IPsec.

The device obtains keys from the GD-quantum server in the following steps:

1. **Connecting the GD-quantum server**—After all commands in IKE GD-quantum view are configured, the device establishes a connection with the specified GD-quantum server.
2. **Logging in to the GD-quantum server**—After the connection is established, the device sends a login request to the GD-quantum server, carrying the GD-quantum access ID and the GD-quantum authentication key. Only devices with verified GD-quantum access IDs and GD-quantum authentication keys can successfully log in to the GD-quantum server.

3. **Obtaining the GD-quantum keys**—After successful login and the IKE phase 1 negotiation, the device obtains the encrypted GD-quantum keys from the GD-quantum server, decrypt them with the GD-quantum decryption keys configured on the device, and finally obtain the GD-quantum keys for IPsec.

When enabling GD-quantum encryption for IKE, the device enters IKE GD-quantum view. Configure the IP address and port number of the GD-quantum server, the GD-quantum access IDs and GD-quantum authentication keys, and the GD-quantum decryption keys in this view.

, Examples

Enable GD-quantum encryption for IKE and enter IKE GD-quantum view.

```
<Sysname> system-view
[Sysname] ike gd-quantum
[Sysname-ike-gdquantum]
```

server-address

Use **server-address** to specify the IP address and port number of the GD-quantum server.

Use **undo server-address** to restore the default.

Syntax

server-address *ip-address* [**port** *port-number*]

undo server-address

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No

Hardware	Command compatibility
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	No

Hardware	Command compatibility
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

No IP address or port number of the GD-quantum server is specified.

Views

IKE GD-quantum view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of the GD-quantum server.

port port-number: Specifies the port number of the GD-quantum server, in the range of 1 to 65535. The default value for the *port-number* argument is 8013.

Usage guidelines

The device interacts with the GD-quantum server specified in this command to obtain the GD-quantum keys. Make sure you specify the IP address and port number that the GD-quantum server actually uses.

Any change to this command does affect the established connection between the device and the GD-quantum server.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the IP address of the GD-quantum server as 192.168.0.111, and the port number as 5656.

```
<Sysname> system-view
```

```
[Sysname] ike gd-quantum
```

```
[Sysname-ike-gdquantum] server-address 192.168.0.111 port 5656
```

New feature: Enabling SNMP notifications for PKI

Enabling SNMP notifications for PKI

About this task

To report critical PKI events to an NMS, enable SNMP notifications for PKI. For PKI notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

Restrictions and guidelines

For the device to generate and output certain types of PKI notifications, enable global PKI notifications and those types of PKI notifications. For the device to stop generating certain types of PKI notifications, disable those types of PKI notifications.

Procedure

1. Enter system view.
system-view
2. Enable SNMP notifications for PKI.
snmp-agent trap enable pki [**ca-cert-invalid** | **ca-cert-valid** | **crl-http-failure** | **crl-http-success** | **crl-invalid** | **crl-ldap-failure** | **crl-ldap-success** | **crl-scep-failure** | **crl-scep-success** | **crl-valid** | **global** | **local-cert-has-expired** | **local-cert-invalid** | **local-cert-ldap-failure** | **local-cert-ldap-success** | **local-cert-nearly-expired** | **local-cert-scep-failure** | **local-cert-scep-success** | **local-cert-valid**] *
By default, SNMP notifications for PKI are disabled.

Command reference

snmp-agent trap enable pki

Use **snmp-agent trap enable pki** to enable SNMP notifications for PKI.

Use **undo snmp-agent trap enable pki** to disable SNMP notifications for PKI.

Syntax

```
snmp-agent trap enable pki [ ca-cert-invalid | ca-cert-valid | crl-http-failure |  
crl-http-success | crl-invalid | crl-ldap-failure | crl-ldap-success | crl-scep-failure |  
crl-scep-success | crl-valid | global | local-cert-has-expired | local-cert-invalid |  
local-cert-ldap-failure | local-cert-ldap-success | local-cert-nearly-expired |  
local-cert-scep-failure | local-cert-scep-success | local-cert-valid ] *  
  
undo snmp-agent trap enable pki [ ca-cert-invalid | ca-cert-valid | crl-http-failure |  
crl-http-success | crl-invalid | crl-ldap-failure | crl-ldap-success | crl-scep-failure |  
crl-scep-success | crl-valid | global | local-cert-has-expired | local-cert-invalid |  
local-cert-ldap-failure | local-cert-ldap-success | local-cert-nearly-expired |  
local-cert-scep-failure | local-cert-scep-success | local-cert-valid ] *
```

Default

SNMP notifications are disabled for PKI.

Views

System view

Predefined user roles

network-admin

Parameters

ca-cert-invalid: Enables notification of invalid CA certificate.

ca-cert-valid: Enables notification of valid CA certificate.

crl-http-failure: Enables notification of failure to obtain CRL through HTTP.

crl-http-success: Enables notification of obtaining CRL successfully through HTTP.

crl-invalid: Enables notification of invalid CRL.

crl-ldap-failure: Enables notification of failure to obtain CRL through LDAP.

crl-ldap-success: Enables notification of obtaining CRL successfully through LDAP.

crl-scep-failure: Enables notification of failure to obtain CRL through SCEP.

crl-scep-success: Enables notification of obtaining CRL successfully through SCEP.

crl-valid: Enables notification of valid CRL.

global: Enables PKI notifications globally.

local-cert-has-expired: Enables notification of local certificate expiration.

local-cert-invalid: Enables notification of invalid local certificate.

local-cert-ldap-failure: Enables notification of failure to obtain local certificate through LDAP.

local-cert-ldap-success: Enables notification of obtaining local certificate successfully through LDAP.

local-cert-nearly-expired: Enables notification of local certificate soon-to-expire.

local-cert-scep-failure: Enables notification of failure to obtain local certificate through SCEP.

local-cert-scep-success: Enables notification of obtaining local certificate successfully through SCEP.

local-cert-valid: Enables notification of valid local certificate.

Usage guidelines

If you do not specify any notification keywords, this command enables all types of PKI notifications. If you specify the notification keywords, this command enables the specified types of PKI notifications.

For the device to generate and output certain types of PKI notifications, enable global PKI notifications and those types of PKI notifications. For the device to stop generating certain types of PKI notifications, disable those types of PKI notifications.

For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable PKI notifications globally.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable pki global
```

Enable notification of invalid CA certificate.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable pki ca-cert-invalid
```

New feature: Configuring the initiator to use dynamic source UDP ports for IKE negotiations

Configuring the initiator to use dynamic source UDP ports for IKE negotiations

1. Enter system view.
system-view
2. Enter IKE profile view.

ike profile *profile-name*

3. Configure the initiator to use dynamic source UDP ports for IKE negotiations.

client source-udp-port dynamic

By default, the source UDP port is 500.

In some scenarios, intermediate devices on the network will drop packets with source UDP port 4500, resulting in IKE negotiation failure. To avoid such failure, you can enable the initiator to use dynamic source UDP ports for IKE negotiations.

Command reference

client source-udp-port dynamic

Use **client source-udp-port dynamic** to configure the initiator to use dynamic source UDP ports for IKE negotiations.

Use **undo client source-udp-port dynamic** to restore the default.

Syntax

client source-udp-port dynamic

undo client source-udp-port dynamic

Default

The source UDP port number used by an initiator for IKE negotiation is 500.

Views

IKE profile view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only on an initiator.

After this command is enabled on an initiator, it uses a random source UDP port number to send IKE negotiation packets. The responder sends packets to the initiator according to the UDP port number in the packets received from the initiator. If the IKE negotiation using the UDP port number fails, the initiator uses another random UDP port number to re-negotiate, and so forth until the IKE negotiation succeeds.

Usually, if a NAT device exists between two IKE peers, IKE will change the source and destination UDP port numbers of the negotiation packets to 4500. In some scenarios, intermediate devices on the network will drop packets with source UDP port 4500, resulting in IKE negotiation failure. To avoid such failure, you can enable the initiator to use dynamic source UDP ports for IKE negotiations.

Modify the configuration of this command does not affect existing IKE SAs.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

In IKE profile **prof1**, enable the initiator to use dynamic UDP port numbers for IKE negotiation.

```
<Sysname> system-view
```

```
[Sysname] ike profile prof1
```

```
[Sysname-ike-profile-prof1] client source-udp-port dynamic
```

Related commands

display ike sa

New feature: Binding a smart token to the device

Binding a smart token to the device

Hardware compatibility with smart token binding

Hardware	Feature compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	Yes
MSR810-SI, MSR810-LM-SI	Yes
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	No

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes

Hardware	Feature compatibility
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Feature compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	No

Hardware	Feature compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Binding the smart token to a PKI domain

About this task

Smart token refers to a third-party hardware device that meets the GM/T 0016-2012 standard, through which out-of-band loading of digital certificates can be realized. If you use this command to bind a smart token to a PKI domain, services (such as SSL or IKE) using the PKI domain can directly

use the local certificate carried in the smart token. The device does not need to request a local certificate from a CA.

Restrictions and guidelines

If a local certificate exists in the PKI domain, the PKI domain does not support binding a smart token.

Procedure

1. Enter system view.
system-view
2. Enter PKI domain view.
pki domain *domain-name*
3. Bind a smart token to the PKI domain.
bind smart-token
By default, no smart token is bound to the PKI domain.

Specifying a user PIN code for the smart token

About this task

After the smart token device is inserted, in encryption, decryption or signature process by using the local certificate carried in the smart token, the device will perform PIN code verification first. If the PIN code specified on the device is inconsistent with the PIN code in the smart token, the digital certificates carried in the smart token cannot be used.

Restrictions and guidelines

You can specify only one user PIN code for the smart token on the device.

Prerequisites

Before specifying a user PIN code for the smart token, contact the administrator of the smart token device to obtain the user PIN code.

Procedure

1. Enter system view.
system-view
2. Specify a user PIN code for the smart token.
pki smart-token user-pin { **cipher** | **simple** } *string*
By default, no user PIN code is specified for the smart token.

Command reference

bind smart-token

Use **bind smart-token** to bind a smart token to a PKI domain.

Use **undo bind** to restore the default.

Syntax

bind smart-token

undo bind

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	Yes
MSR810-SI, MSR810-LM-SI	Yes
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	No

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	No

Hardware	Command compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

No smart token is bound to a PKI domain.

Views

PKI domain view

Predefined user roles

network-admin

Usage guidelines

Smart token refers to a third-party hardware device that meets the GM/T 0016-2012 standard, through which out-of-band loading of digital certificates can be realized. If you use this command to bind a smart token to a PKI domain, services (such as SSL or IKE) using the PKI domain can directly use the local certificate carried in the smart token. The device does not need to request a local certificate from a CA.

If a local certificate exists in the PKI domain, the PKI domain does not support binding a smart token.

Examples

Bind a smart token to PKI domain **aaa**.

```
<Sysname> system-view
[Sysname] pki domain aaa
```

[Sysname-pki-domain-aaa] bind smart-token

Related commands

display pki certificate domain

display pki smart-token

Use **display pki smart-token** to display smart token information on a device.

Syntax

display pki smart-token

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes
MSR810-LMS, MSR810-LUS	Yes
MSR810-SI, MSR810-LM-SI	Yes
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	No

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes

Hardware	Command compatibility
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	No
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	No

Hardware	Command compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the brief information of the digital certificates carried in the inserted smart token device.

Examples

Display smart token information on a device.

```
<Sysname> display pki smart-token
    Signature certificate:
      Serial number:
        1a:10:00:00:00:00:01:1e:b7:84
      Issuer: C=CN, CN=TESTSM2CA
      Subject: C=CN, CN=TESTSM2
    Encryption certificate:
      Serial number:
        1a:10:00:00:00:00:01:1e:bf:54
      Issuer: C=CN, CN=TESTSM2CA
      Subject: C=CN, CN=TESTSM2
```

Table 104 Command Output

Field	Description
Signature certificate	Signature certificate details.
Serial number	Certificate serial number.
Issuer	Certificate issuer.
Subject	Entity to which the certificate belongs.
Encryption certificate	Encryption certificate details.

Related commands

display pki certificate domain

pki smart-token

Use **pki smart-token** to specify a user PIN code for the smart token.

Use **undo pki smart-token** to restore the default.

Syntax

pki smart-token user-pin { cipher | simple } *string*

undo pki smart-token

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	Yes

Hardware	Command compatibility
MSR810-LMS, MSR810-LUS	Yes
MSR810-SI, MSR810-LM-SI	Yes
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	No
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	No
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	No
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	No

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	Yes
MSR830-4LM-WiNet	Yes
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	Yes
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	No
MSR2600-6-WiNet	No
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	No
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	Yes
MSR860-6HI-XS	No

Hardware	Command compatibility
MSR2630-XS	No
MSR3600-28-XS	No
MSR3610-XS	No
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	No
MSR3640-XS	No
MSR3660-XS	No

Hardware	Command compatibility
MSR810-LM-GL	Yes
MSR810-W-LM-GL	Yes
MSR830-6EI-GL	Yes
MSR830-10EI-GL	Yes
MSR830-6HI-GL	No
MSR830-10HI-GL	No
MSR1004S-5G-GL	No
MSR2600-6-X1-GL	No
MSR3600-28-SI-GL	No

Default

No user PIN code is specified for the smart token.

Views

System view

Predefined user roles

network-admin

Parameters

user-pin: Specifies a user PIN code for the smart token.

cipher: Specifies the user PIN code in encrypted form.

simple: Specifies the user PIN code in plaintext form.

string: Specifies the user PIN code. The plaintext form is a case-sensitive string of 1 to 31 characters. The encrypted form is a case-sensitive string of 1 to 73 characters.

Usage guidelines

After the smart token device is inserted, in encryption, decryption or signature process by using the local certificate carried in the smart token, the device will perform PIN code verification first. If the PIN code specified on the device is inconsistent with the PIN code in the smart token, the digital certificates carried in the smart token cannot be used.

Before specifying a user PIN code for the smart token, contact the administrator of the smart token device to obtain the user PIN code.

You can specify only one user PIN code for the smart token on the device. If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Specify user PIN code 123456 for the smart token.  
<Sysname> system-view  
[Sysname] pki smart-token user-pin simple 123456
```

New feature: Configuring the title for the PKI entity

Configuring the title for the PKI entity

1. Enter system view.
system-view
2. Create a PKI entity and enter its view.
pki entity *entity-name*
3. Configure the title for the PKI entity.
title *title*
By default, the title for the PKI entity is not configured.

Command reference

title

Use **title** to configure a title for a PKI entity.

Use **undo title** to restore the default.

Syntax

```
title title  
undo title
```

Default

No title is configured for a PKI entity.

Views

PKI entity view

Predefined user roles

network-admin

Parameters

title: Specifies a title, a case-insensitive string of 1 to 63 characters.

Usage guidelines

By default, a PKI entity does not include the title attribute. This attribute is defined in international standard ITU-T X.520. You can use this command to configure the title of a PKI entity.

Examples

```
# Configure title manager for PKI entity entity1 (for example, Manager John).
<Sysname> system-view
[Sysname] pki entity entity1
[Sysname-pki-entity-entity1] title manager
```

New feature: Configuring ZD-quantum encryption

Configuring ZD-quantum encryption

About this task

After you enable ZD-quantum encryption for IKE, the device can use the symmetric key provided by the ZD-quantum key service platform to encrypt the IPsec protected data, which further enhance the security of IPsec.

The device obtains keys from the ZD-quantum key service platform in the following steps:

1. **Connecting the ZD-quantum key service platform**—After all commands in IKE ZD-quantum view are configured, the device establishes a connection to the specified ZD-quantum key service platform through the SIM key.
2. **Logging in to the ZD-quantum key service platform**—After the connection is established, the device sends a login request to the ZD-quantum key service platform, carrying the unique ZD-quantum access ID. Only devices with verified ZD-quantum access IDs can successfully log in to the ZD-quantum key service platform.
3. **Obtaining the ZD-quantum keys**—After successful login and the IKE phase 1 negotiation, the device obtains the encrypted ZD-quantum keys from the ZD-quantum key service platform, decrypts them with the key in the SIM key inserted into the device, and finally obtains the ZD-quantum keys for IPsec.

Hardware and feature compatibility

Hardware	Feature compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	Yes
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No

Hardware	Feature compatibility
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Feature compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Feature compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	Yes
MSR2630-XS	Yes
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Feature compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	No

Restrictions and guidelines

This feature is only available for IKEv1 main mode negotiation.

This feature is only supported on devices with the SIC-4G/5G function. You must install the ZD-quantum SIM card in the SIC-4G/5G SIM card slot. For more information about SIC-4G/5G, see the installation guide.

Procedure

1. Enter system view.

system-view

2. Enable ZD-quantum encryption for IKE and enter IKE ZD-quantum view.

ike zd-quantum

By default, ZD-quantum encryption for IKE is disabled.

3. Specify a ZD-quantum access ID.

app-dev-info *app-dev-info*

By default, no ZD-quantum access ID is specified and the ZD-quantum access ID is defined by the administrator.

Command reference

app-dev-info (IKE ZD-quantum view)

Use **app-dev-info** to specify a ZD-quantum access ID.

Use **undo app-dev-info** to restore the default.

Syntax

app-dev-info *app-dev-info*

undo app-dev-info

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK,	No

Hardware	Command compatibility
MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	Yes
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No

Hardware	Command compatibility
MSR860-6HI-XS	Yes
MSR2630-XS	Yes
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	No

Default

No ZD-quantum access ID is specified.

Views

IKE ZD-quantum view

Predefined user roles

network-admin

Parameters

app-dev-info: Specifies a ZD-quantum access ID, a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can specify ZD-quantum access IDs for devices. Make sure the ZD-quantum access ID for a device is unique. If the ZD-quantum access IDs configured on both IKE ends are not unique, the device cannot obtain the quantum key. After the device is connected to the ZD-quantum key service platform, you can use the ZD-quantum access ID to login in to the ZD-quantum key service platform.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify ZD-quantum access ID **devicea**.

```
<Sysname> system-view
```

```
[Sysname] ike zd-quantum
[Sysname-ike-zdquantum] app-dev-info devicea
```

ike zd-quantum

Use **ike gd-quantum** to enable ZD-quantum encryption for IKE and enter IKE ZD-quantum view.

Use **undo ike gd-quantum** to disable ZD-quantum encryption for IKE.

Syntax

ike zd-quantum

undo ike zd-quantum

The following compatibility matrixes show the support of hardware platforms for this command:

Hardware	Command compatibility
MSR610	No
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	No
MSR810-LMS, MSR810-LUS	No
MSR810-SI, MSR810-LM-SI	No
MSR810-LMS-EA, MSR810-LME	No
MSR1004S-5G, MSR1004S-5G-CN	Yes
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	No
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	Yes
MSR2600-10-X1	No
MSR2630	No
MSR3600-28, MSR3600-51	No
MSR3600-28-SI, MSR3600-51-SI	No
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	No
MSR3600-28-G-DP, MSR3600-51-G-DP	No
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	No
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	Yes
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	No
MSR3610-G, MSR3620-G	No
MSR3640-G	No
MSR3640-X1-HI	Yes

Hardware	Command compatibility
MSR810-W-WiNet, MSR810-LM-WiNet	No
MSR830-4LM-WiNet	No
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	No
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	Yes
MSR2600-6-WiNet	Yes
MSR2600-10-X1-WiNet	No
MSR2630-WiNet	No
MSR3600-28-WiNet	No
MSR3610-X1-WiNet	Yes
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	No

Hardware	Command compatibility
MSR860-6EI-XS	No
MSR860-6HI-XS	Yes
MSR2630-XS	Yes
MSR3600-28-XS	No
MSR3610-XS	Yes
MSR3620-XS	No
MSR3610-I-XS	No
MSR3610-IE-XS	No
MSR3620-X1-XS	Yes
MSR3640-XS	Yes
MSR3660-XS	Yes

Hardware	Command compatibility
MSR810-LM-GL	No
MSR810-W-LM-GL	No
MSR830-6EI-GL	No
MSR830-10EI-GL	No
MSR830-6HI-GL	Yes
MSR830-10HI-GL	Yes
MSR1004S-5G-GL	Yes
MSR2600-6-X1-GL	Yes
MSR3600-28-SI-GL	No

Default

ZD-quantum encryption for IKE is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Operating mechanism

After you enable ZD-quantum encryption for IKE, the device can use the symmetric key provided by the ZD-quantum key service platform to encrypt the IPsec protected data, which further enhance the security of IPsec.

The device obtains keys from the ZD-quantum key service platform in the following steps:

1. **Connecting the ZD-quantum key service platform**—After all commands in IKE ZD-quantum view are configured, the device establishes a connection to the specified ZD-quantum key service platform through the SIM key.
2. **Logging in to the ZD-quantum key service platform**—After the connection is established, the device sends a login request to the ZD-quantum key service platform, carrying the unique ZD-quantum access ID. Only devices with verified ZD-quantum access IDs can successfully log in to the ZD-quantum key service platform.
3. **Obtaining the ZD-quantum keys**—After successful login and the IKE phase 1 negotiation, the device obtains the encrypted ZD-quantum keys from the ZD-quantum key service platform, decrypts them with the key in the SIM key inserted into the device, and finally obtains the ZD-quantum keys for IPsec.

Restrictions and guidelines

This command is only available for IKEv1 main mode negotiation.

This command is only supported on devices with the SIC-4G/5G function. You must install the ZD-quantum SIM key on the SIC-4G/5G SIM card slot. For more information about SIC-4G/5G, see the installation guide.

Examples

```
# Enable ZD-quantum encryption for IKE and enter IKE ZD-quantum view.
```

```
<Sysname> system-view  
[Sysname] ike zd-quantum  
[Sysname-ike-zdquantum]
```

New feature: Setting a limit to the number of IKEv2 SAs

Setting a limit to the number of IKEv2 SAs

About this task

You can use this feature to limit the maximum number of negotiating IKEv2 SAs.

The supported maximum number of negotiating IKEv2 SAs depends on the device's processing capability. Adjust the maximum number of negotiating IKEv2 SAs to make full use of the device's processing capability without affecting the IKEv2 SA negotiation efficiency.

Procedure

1. Enter system view.
system-view
2. Set a limit to the number of IKEv2 SAs.
ikev2 limit max-negotiating-sa *negotiation-limit*
By default, no limit is set to the number of IKEv2 SAs.

Command reference

ikev2 limit

Use **ikev2 limit** to set limit to the number of IKEv2 SAs.

Use **undo ikev2 limit** to restore the default.

Syntax

ikev2 limit max-negotiating-sa *negotiation-limit*

undo ikev2 limit max-negotiating-sa

Default

No limit is set to the number of IKEv2 SAs.

Views

System view

Predefined user roles

network-admin

Parameters

max-negotiating-sa *negotiation-limit*: Specifies the maximum number of negotiating IKEv2 SAs.
The value range for the *negotiation-limit* argument is 1 to 99999.

Usage guidelines

The supported maximum number of negotiating IKEv2 SAs depends on the device's processing capability. Adjust the maximum number of negotiating IKEv2 SAs to make full use of the device's processing capability without affecting the IKEv2 SA negotiation efficiency.

Examples

Set the maximum number of negotiating IKEv2 SAs to 200.

```
<Sysname> system-view
```

```
[Sysname] ikev2 limit max-negotiating-sa 200
```

Modified feature: Displaying information about IPsec SAs

Feature change description

As from this release, the **display ipsec sa** command supports displaying the **local address/port** and **remote address/port** fields.

Command changes

Modified command: display ipsec sa

Use **display ipsec sa** to display information about IPsec SAs.

Syntax

```
display ipsec sa [ brief | count | interface interface-type interface-number [ brief | count ]  
| { ipv6-policy | policy } policy-name [ seq-number ] [ brief | count ] | profile  
profile-name [ brief | count ] | remote [ ipv6 ] ip-address [ brief | count ] ]
```

Views

Any view

Change description

Before modification: The **local address/port** and **remote address/port** fields were not displayed in the output for this command.

```
<Sysname> display ipsec sa  
-----  
Interface: GigabitEthernet1/0/1  
-----  
  
-----  
IPsec policy: r2  
Sequence number: 1  
Alias: mypolicy  
Mode: ISAKMP  
-----  
  
Tunnel id: 3  
Encapsulation mode: tunnel  
Perfect Forward Secrecy:  
Inside VPN: vp1  
Extended Sequence Numbers enable: Y  
Traffic Flow Confidentiality enable: N  
Transmitting entity: Initiator  
Path MTU: 1443  
Tunnel:  
    local  address: 2.2.2.2  
    remote address: 1.1.1.2  
Flow:  
    sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip  
    dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip  
  
[Inbound ESP SAs]  
    SPI: 3564837569 (0xd47b1ac1)  
    Connection ID: 90194313219  
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1  
    SA duration (kilobytes/sec): 4294967295/604800  
    SA remaining duration (kilobytes/sec): 1843200/2686
```

Max received sequence-number: 5
Anti-replay check enable: Y
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]

SPI: 801701189 (0x2fc8fd45)
Connection ID: 64424509441
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 4294967295/604800
SA remaining duration (kilobytes/sec): 1843200/2686
Max sent sequence-number: 6
UDP encapsulation used for NAT traversal: N
Status: Active

After modification: The **local address/port** and **remote address/port** fields are displayed in the output for this command.

<Sysname> display ipsec sa

Interface: GigabitEthernet1/0/1

IPsec policy: r2
Sequence number: 1
Alias: mypolicy
Mode: ISAKMP

Tunnel id: 3
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN: vp1
Extended Sequence Numbers enable: Y
Traffic Flow Confidentiality enable: N
Transmitting entity: Initiator
Path MTU: 1443
Tunnel:

local address/port: 2.2.2.2/500
remote address/port: 1.1.1.2/500

Flow:

sour addr: 192.168.2.0/255.255.255.0 port: 0 protocol: ip
dest addr: 192.168.1.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 3564837569 (0xd47blac1)
Connection ID: 90194313219
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 4294967295/604800

```
SA remaining duration (kilobytes/sec): 1843200/2686
Max received sequence-number: 5
Anti-replay check enable: Y
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N
Status: Active
```

[Outbound ESP SAs]

```
SPI: 801701189 (0x2fc8fd45)
Connection ID: 64424509441
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 4294967295/604800
SA remaining duration (kilobytes/sec): 1843200/2686
Max sent sequence-number: 6
UDP encapsulation used for NAT traversal: N
Status: Active
```

Table 105 Command output

Field	Description
local address/port	Local end IP address and port number of the IPsec tunnel.
remote address/port	Remote end IP address and port number of the IPsec tunnel.

Modified feature: Configuring a peer ID for IKE profile matching

Feature change description

As from this release, the device supports specifying the host name of the peer when you configure a peer ID for IKE profile matching.

Command changes

Modified command: match remote

Use **match remote** to configure a peer ID for IKE profile matching.

Use **undo match remote** to delete a peer ID for IKE profile matching.

Old syntax

```
match remote { certificate policy-name | identity { address { { ipv4-address [ mask | mask-length ] | range low-ipv4-address high-ipv4-address } | ipv6 { ipv6-address [ prefix-length ] | range low-ipv6-address high-ipv6-address } } } [ vpn-instance vpn-instance-name ] | fqdn fqdn-name | user-fqdn user-fqdn-name | domain fqdn-domain-name } }
```

```
undo match remote { certificate policy-name | identity { address { { ipv4-address [ mask | mask-length ] | range low-ipv4-address high-ipv4-address } | ipv6 { ipv6-address
```



```
[ prefix-length ] | range low-ipv6-address high-ipv6-address } } [ vpn-instance
vpn-instance-name ] | fqdn fqdn-name | user-fqdn user-fqdn-name | domain
fqdn-domain-name } }
```

New syntax

```
match remote { certificate policy-name | identity { address { { ipv4-address [ mask |
mask-length ] | hostname host-name | range low-ipv4-address high-ipv4-address } | ipv6
{ ipv6-address [ prefix-length ] | range low-ipv6-address high-ipv6-address } } }
[ vpn-instance vpn-instance-name ] | fqdn fqdn-name | user-fqdn user-fqdn-name |
domain fqdn-domain-name } }
```

```
undo match remote { certificate policy-name | identity { address { { ipv4-address [ mask |
mask-length ] | hostname host-name | range low-ipv4-address high-ipv4-address } | ipv6
{ ipv6-address [ prefix-length ] | range low-ipv6-address high-ipv6-address } } }
[ vpn-instance vpn-instance-name ] | fqdn fqdn-name | user-fqdn user-fqdn-name |
domain fqdn-domain-name } }
```

Views

IKE profile view

Change description

The **address hostname** *host-name* option is added to specify the host name of the peer, which is a case-insensitive string of 1 to 253 characters.

The following usage guidelines for this command are added:

The local device resolves the host name to an IP address as follows:

- If a DNS server that supports DDNS is used for resolution, the local device queries the remote IP address from the DNS server. When the remote IP address changes, the remote device (as a DDNS client) sends a request to the DDNS server to update the host name and IP address mapping. The DDNS server then inform the DNS server to update the DNS entry accordingly. This mechanism ensures that the local device can always obtain the latest remote IP address.
- If a static DNS entry (configured by using the **ip host** command) is used for resolution, you must update the DNS entry whenever the remote IP address changes. After the old DNS entry expires, the newly configured DNS entry applies to the resolution.

For example, the local end has a static DNS entry which maps the host name **test** to the IP address 1.1.1.1. Configure the following commands:

In IKE keychain **keychain1**, configure a preshared key and specify the peer address by specifying host name **test**.

```
[Sysname] ike profile profile1
```

```
[Sysname-ike-profile-profile1] match remote identity address hostname test
```

Change the IP address for the host **test** to 2.2.2.2.

```
[Sysname] ip host test 2.2.2.2
```

In this case, the local end obtains the latest IP address of the remote host, which is 2.2.2.2. For more information about DNS, see *Layer 3—IP Services Command Reference*.

Modified feature: Configuring a preshared key

Feature change description

As from this release, the device supports specifying the host name of the peer when you configure a preshared key.

Command changes

Modified command: pre-shared-key

Use **pre-shared-key** to configure a preshared key.

Use **undo pre-shared-key** to delete a preshared key.

Old syntax

In non-FIPS mode:

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key { cipher | simple } string
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

In FIPS mode:

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key [ cipher string ]
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

New syntax

In non-FIPS mode:

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | hostname host-name | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key { cipher | simple } string
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | hostname host-name | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

In FIPS mode:

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | hostname host-name | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key [ cipher string ]
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | hostname host-name | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

Views

IKE keychain view

Change description

The **address hostname** *host-name* option is added to specify the host name of the peer, which is a case-insensitive string of 1 to 253 characters.

The following usage guidelines for this command are added:

The address option or the hostname option specifies the peer with which the device can use the preshared key to perform IKE negotiation. If the IP address or the FQDN of the peer matches the criteria configured by this command, the pre-shared key is used in IKE negotiation.

The local device resolves the host name to an IP address as follows:

- If a DNS server that supports DDNS is used for resolution, the local device queries the remote IP address from the DNS server. When the remote IP address changes, the remote device (as a DDNS client) sends a request to the DDNS server to update the host name and IP address mapping. The DDNS server then inform the DNS server to update the DNS entry accordingly. This mechanism ensures that the local device can always obtain the latest remote IP address.
- If a static DNS entry (configured by using the **ip host** command) is used for resolution, you must update the DNS entry whenever the remote IP address changes. After the old DNS entry expires, the newly configured DNS entry applies to the resolution.

For example, the local end has a static DNS entry which maps the host name **test** to the IP address 1.1.1.1. Configure the following commands:

In IKE keychain **keychain1**, configure a preshared key and specify the peer address by specifying host name **test**.

```
[Sysname] ike keychain keychain1
```

```
[Sysname-ike-keychain-keychain1] pre-shared-key address hostname test key simple 123456
```

Change the IP address for the host **test** to 2.2.2.2.

```
[Sysname] ip host test 2.2.2.2
```

In this case, the local end obtains the latest IP address of the remote host, which is 2.2.2.2. For more information about DNS, see *Layer 3—IP Services Command Reference*.

Modified feature: Enabling ALG to process IP fragments and TCP segments

Feature change description

As from this release, ALG supports processing IP fragments and TCP segments.

Command changes

Modified command: session alg fragment

Use **session alg fragment** to enable ALG to process IP fragments and TCP segments.

Use **undo session alg fragment** to disable ALG from processing IP fragments and TCP segments.

Syntax

session alg fragment sip

undo session alg fragment sip

Views

System view

Change description

Before modification:

Use **session alg fragment** to enable ALG to process fragments.

Use **undo session alg fragment** to disable ALG from processing fragments.

By default, ALG does not process fragments.

sip: Specifies fragments of SIP.

After modification:

Use **session alg fragment** to enable ALG to process IP fragments and TCP segments.

Use **undo session alg fragment** to disable ALG from processing IP fragments and TCP segments.

By default, ALG does not process IP fragments and TCP segments.

sip: Specifies IP fragments and TCP segments.

Modified feature: Not support for DES, 3DES, MD5, RC4, and RC2 cipher suites in SSL client and server policies

Feature change description

By default, the SSL client policies and SSL server policies on the following devices do not support DES, 3DES, MD5, RC4, and RC2 cipher suites: MSR610, MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN, MSR3600-28-G-DP, MSR3600-51-G-DP, MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1, MSR3640-G, MSR3640-X1-HI, MSR3610-X1-WiNet, MSR3610-XS, MSR3620-X1-XS, MSR3640-XS, MSR3660-XS.

Command changes

Modified command: ciphersuite

Use **ciphersuite** to specify the cipher suites supported by an SSL server policy.

Use **undo ciphersuite** to restore the default.

Syntax

In non-FIPS mode:

ciphersuite	{	dhe_rsa_aes_128_cbc_sha		dhe_rsa_aes_128_cbc_sha256	
dhe_rsa_aes_256_cbc_sha				dhe_rsa_aes_256_cbc_sha256	
ecdhe_ecdsa_aes_128_cbc_sha256				ecdhe_ecdsa_aes_128_gcm_sha256	
ecdhe_ecdsa_aes_256_cbc_sha384				ecdhe_ecdsa_aes_256_gcm_sha384	
ecdhe_rsa_aes_128_cbc_sha256				ecdhe_rsa_aes_128_gcm_sha256	
ecdhe_rsa_aes_256_cbc_sha384				ecdhe_rsa_aes_256_gcm_sha384	

```

rsa_3des_edc_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 |
rsa_aes_128_gcm_sha256 | rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 |
rsa_aes_256_gcm_sha384 | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha |
tls_aes_128_ccm_sha256 | tls_aes_128_ccm_8_sha256 | tls_aes_128_gcm_sha256 |
tls_aes_256_gcm_sha384 | tls_chacha20_poly1305_sha256 } * <1-11>

```

undo ciphersuite

In FIPS mode:

```

ciphersuite { ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_256_cbc_sha384
| ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_gcm_sha384 |
ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 |
ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_256_gcm_sha384 |
rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 | rsa_aes_128_gcm_sha256 |
rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 | rsa_aes_256_gcm_sha384 }
* <1-11>

```

undo ciphersuite

Views

SSL server policy view

Change description

Before modification: By default, an SSL server policy supports all cipher suites.

After modification: The default settings vary by device model, as shown in the following tables:

Hardware	Default
MSR610	- In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	An SSL server policy supports all cipher suites.
MSR810-LMS, MSR810-LUS	An SSL server policy supports all cipher suites.
MSR810-SI, MSR810-LM-SI	An SSL server policy supports all

Hardware	Default
	cipher suites.
MSR810-LMS-EA, MSR810-LME	An SSL server policy supports all cipher suites.
MSR1004S-5G, MSR1004S-5G-CN	An SSL server policy supports all cipher suites.
	- In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR1104S-W, MSR1104S-5G-CN, MSR1104S-W-5G-CN, MSR1104S-W-CAT6,	
MSR2600-6-X1, MSR2600-15-X1-T	An SSL server policy supports all cipher suites.
MSR2600-10-X1	An SSL server policy supports all cipher suites.
MSR2630	An SSL server policy supports all cipher suites.
MSR3600-28, MSR3600-51	An SSL server policy supports all cipher suites.
MSR3600-28-SI, MSR3600-51-SI	An SSL server policy supports all cipher suites.
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	An SSL server policy supports all cipher suites.
MSR3600-28-G-DP, MSR3600-51-G-DP	- In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_

Hardware	Default
	md5
	- rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	An SSL server policy supports all cipher suites. - In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	An SSL server policy supports all cipher suites. - In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	An SSL server policy supports all cipher suites. - In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR3610-G, MSR3620-G	An SSL server policy supports all cipher suites. - In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR3640-G	An SSL server policy supports all cipher suites. - In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.
MSR3640-X1-HI	An SSL server policy supports all cipher suites. - In non-FIPS mode, an SSL server policy supports all cipher suites except the following: - rsa_3des_edc_cbc_sha - rsa_des_cbc_sha - rsa_rc4_128_md5 - rsa_rc4_128_sha - In FIPS mode, an SSL server policy supports all cipher suites.

Hardware	Default
	mode, an SSL server policy supports all cipher suites except the following: ○ rsa_3des_edc_cbc_sha ○ rsa_des_cbc_sha ○ rsa_rc4_128_md5 ○ rsa_rc4_128_sha • In FIPS mode, an SSL server policy supports all cipher suites.

Hardware	Default
MSR810-W-WiNet, MSR810-LM-WiNet	An SSL server policy supports all cipher suites.
MSR830-4LM-WiNet	An SSL server policy supports all cipher suites.
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	An SSL server policy supports all cipher suites.
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	An SSL server policy supports all cipher suites.
MSR2600-6-WiNet	An SSL server policy supports all cipher suites.
MSR2600-10-X1-WiNet	An SSL server policy supports all cipher suites.
MSR2630-WiNet	An SSL server policy supports all cipher suites.
MSR3600-28-WiNet	An SSL server policy supports all cipher suites. • In non-FIPS mode, an SSL server policy supports all cipher suites except the following:
MSR3610-X1-WiNet	○ rsa_3des_edc_cbc_sha ○ rsa_des_cbc_sha

Hardware	Default
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	○ rsa_rc4_128_md5 ○ rsa_rc4_128_sha • In FIPS mode, an SSL server policy supports all cipher suites.
	An SSL server policy supports all cipher suites.

Hardware	Default
MSR860-6EI-XS	An SSL server policy supports all cipher suites.
MSR860-6HI-XS	An SSL server policy supports all cipher suites.
MSR2630-XS	An SSL server policy supports all cipher suites.
MSR3600-28-XS	An SSL server policy supports all cipher suites.
MSR3610-XS	• In non-FIPS mode, an SSL server policy supports all cipher suites except the following: ○ rsa_3des_ede_cbc_sha ○ rsa_des_cbc_sha ○ rsa_rc4_128_md5 ○ rsa_rc4_128_sha • In FIPS mode, an SSL server policy supports all cipher suites.
	An SSL server policy supports all cipher suites.
	An SSL server policy supports all cipher suites.
	An SSL server policy supports all cipher suites.
	An SSL server policy supports all cipher suites.
MSR3620-XS	An SSL server policy supports all cipher suites.
MSR3610-I-XS	An SSL server policy supports all cipher suites.
MSR3610-IE-XS	An SSL server policy supports all cipher suites.
MSR3620-X1-XS	• In non-FIPS

Hardware	Default
	mode, an SSL server policy supports all cipher suites except the following: ○ rsa_3des_edc_cbc_sha ○ rsa_des_cbc_sha ○ rsa_rc4_128_md5 ○ rsa_rc4_128_sha • In FIPS mode, an SSL server policy supports all cipher suites. • In non-FIPS mode, an SSL server policy supports all cipher suites except the following: ○ rsa_3des_edc_cbc_sha ○ rsa_des_cbc_sha ○ rsa_rc4_128_md5 ○ rsa_rc4_128_sha • In FIPS mode, an SSL server policy supports all cipher suites. • In non-FIPS mode, an SSL server policy supports all cipher suites except the following: ○ rsa_3des_edc_cbc_sha ○ rsa_des_cbc_sha ○ rsa_rc4_128_md5 ○ rsa_rc4_128_sha • In FIPS mode, an SSL server policy supports all cipher suites.
MSR3640-XS	
MSR3660-XS	

Hardware	Default
MSR810-LM-GL	An SSL server policy supports all cipher suites.
MSR810-W-LM-GL	An SSL server policy supports all cipher suites.
MSR830-6EI-GL	An SSL server policy supports all cipher suites.
MSR830-10EI-GL	An SSL server policy supports all cipher suites.
MSR830-6HI-GL	An SSL server policy supports all cipher suites.
MSR830-10HI-GL	An SSL server policy supports all cipher suites.
MSR1004S-5G-GL	An SSL server policy supports all cipher suites.
MSR2600-6-X1-GL	An SSL server policy supports all cipher suites.
MSR3600-28-SI-GL	An SSL server policy supports all cipher suites.

Modified command: prefer-cipher

Use **prefer-cipher** to specify a preferred cipher suite for an SSL client policy.

Use **undo prefer-cipher** to restore the default.

Syntax

In non-FIPS mode:

```
prefer-cipher {  dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_128_cbc_sha256 |
dhe_rsa_aes_256_cbc_sha | dhe_rsa_aes_256_cbc_sha256 |
ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_128_gcm_sha256 |
ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_256_gcm_sha384 |
ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 |
ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_256_gcm_sha384 |
rsa_3des_edc_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 |
rsa_aes_128_gcm_sha256 | rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 |
rsa_aes_256_gcm_sha384 | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha |
tls_aes_128_ccm_sha256 | tls_aes_128_ccm_8_sha256 | tls_aes_128_gcm_sha256 |
tls_aes_256_gcm_sha384 | tls_chacha20_poly1305_sha256 } * <1-11>
```

undo prefer-cipher

In FIPS mode:

```

prefer-cipher { ecdhe_ecdsa_aes_128_cbc_sha256 |
ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_cbc_sha384 |
ecdhe_ecdsa_aes_256_gcm_sha384 | ecdhe_rsa_aes_128_cbc_sha256 |
ecdhe_rsa_aes_128_gcm_sha256 | ecdhe_rsa_aes_256_cbc_sha384 |
ecdhe_rsa_aes_256_gcm_sha384 | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 |
rsa_aes_128_gcm_sha256 | rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 |
rsa_aes_256_gcm_sha384 } * <1-11>

```

undo prefer-cipher

Views

SSL client policy view

Change description

Before modification:

- In non-FIPS mode:
The preferred cipher suites of an SSL client policy are **dhe_rsa_aes_256_cbc_sha**, **rsa_aes_256_cbc_sha**, **dhe_rsa_aes_128_cbc_sha**, **rsa_aes_128_cbc_sha**, and **rsa_3des_cbc_sha**.
- In FIPS mode:
The preferred cipher suites of an SSL client policy are **rsa_aes_256_cbc_sha**, **rsa_aes_128_cbc_sha**, and **rsa_3des_cbc_sha**.

After modification:

- In FIPS mode:
The preferred cipher suites of an SSL client policy are **rsa_aes_256_cbc_sha** and **rsa_aes_128_cbc_sha**.
- In non-FIPS mode:
The default settings vary by device model, as shown in the following tables:

Hardware	Default
MSR610	The preferred cipher suites of an SSL client policy are the following: the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR810-LMS, MSR810-LUS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha

Hardware	Default
MSR810-SI, MSR810-LM-SI	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR810-LMS-EA, MSR810-LME	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR1004S-5G, MSR1004S-5G-CN	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2600-10-X1	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2630	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28, MSR3600-51	The preferred cipher suites of an SSL

Hardware	Default
	client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28-SI, MSR3600-51-SI	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28-G-DP, MSR3600-51-G-DP	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3610-G, MSR3620-G	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha

Hardware	Default
	•rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3640-G	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3640-X1-HI	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha

Hardware	Default
MSR810-W-WiNet, MSR810-LM-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-4LM-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2600-6-WiNet	The preferred cipher suites of an SSL

Hardware	Default
	client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2600-10-X1-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2630-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3610-X1-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha

Hardware	Default
MSR860-6EI-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha

Hardware	Default
MSR860-6HI-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2630-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3610-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3620-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3610-I-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3610-IE-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3620-X1-XS	The preferred cipher suites of an SSL

Hardware	Default
	client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3640-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha
MSR3660-XS	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha

Hardware	Default
MSR810-LM-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR810-W-LM-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-6EI-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-10EI-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-6HI-GL	The preferred cipher suites of an SSL client policy are the following:

Hardware	Default
	•dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR830-10HI-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR1004S-5G-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR2600-6-X1-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha
MSR3600-28-SI-GL	The preferred cipher suites of an SSL client policy are the following: •dhe_rsa_aes_256_cbc_sha •rsa_aes_256_cbc_sha •dhe_rsa_aes_128_cbc_sha •rsa_aes_128_cbc_sha •rsa_3des_edc_cbc_sha

Modified feature: Not support for an SSL protocol version lower than TLS 1.1 for session negotiation

Feature change description

By default, the SSL client policies and SSL server policies on the following devices do not use an SSL protocol version lower than TLS 1.1 for session negotiation: MSR610, MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN, MSR3600-28-G-DP, MSR3600-51-G-DP, MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1, MSR3640-G, MSR3640-X1-HI, MSR3610-X1-WiNet, MSR3610-XS, MSR3620-X1-XS, MSR3640-XS, and MSR3660-XS.

If the security enhanced level is set to 2, the following rules apply:

- SSL client policies and SSL server policies do not support cipher suites that contain DES, 3DES, MD5, RC4, and RC2.
- SSL client policies and SSL server policies do not support SSL protocol versions lower than TLS 1.1.
- SSL session renegotiation cannot be enabled.

Command changes

Modified command: `ssl version disable`

Use **`ssl version disable`** to disable the SSL server from using specific SSL protocol versions for session negotiation.

Use **`undo ssl version disable`** restore the default.

Syntax

In non-FIPS mode:

`ssl version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 | tls1.3 } * disable`

`undo ssl version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 | tls1.3 } * disable`

In FIPS mode:

`ssl version { tls1.0 | tls1.1 | tls1.2 } * disable`

`undo ssl version { tls1.0 | tls1.1 | tls1.2 } * disable`

Views

System view

Change description

Before modification:

- In non-FIPS mode:
The SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
- In FIPS mode:
The SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

After modification: The default settings vary by device model, as shown in the following tables:

Hardware	Default
MSR610	• In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI,	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0,

Hardware	Default
MSR810-LM-EA, MSR810-LM-EI	TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR810-LMS, MSR810-LUS	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR810-SI, MSR810-LM-SI	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR810-LMS-EA, MSR810-LME	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR1004S-5G, MSR1004S-5G-CN	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

Hardware	Default
MSR1104S-W, MSR1104S-5G-CN, MSR1104S-W-5G-CN	• In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.
MSR2600-6-X1, MSR2600-15-X1-T	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR2600-10-X1	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR2630	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR3600-28, MSR3600-51	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server

Hardware	Default
MSR3600-28-SI, MSR3600-51-SI	- supports TLS 1.0, TLS 1.1, and TLS 1.2. - In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR3600-28-G-DP, MSR3600-51-G-DP	- In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	- In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode,

Hardware	Default
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	- the SSL server supports TLS 1.1 and TLS 1.2. - In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR3610-G, MSR3620-G	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR3640-G	- In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.
MSR3640-X1-HI	- In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.

Hardware	Default
MSR810-W-WiNet, MSR810-LM-WiNet	In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS

Hardware	Default
MSR830-4LM-WiNet	1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. - In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. - In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	- In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. - In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	- In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. - In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR2600-6-WiNet	In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR2600-10-X1-WiNet	In non-FIPS

Hardware	Default
	mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR2630-WiNet	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR3600-28-WiNet	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3.
MSR3610-X1-WiNet	• In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR3610-WiNet, MSR3620-10-WiNet, MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1,

Hardware	Default

and TLS 1.2.

Hardware	Default

MSR860-6EI-XS

- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
- In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

MSR860-6HI-XS

- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
- In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

MSR2630-XS

- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
- In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

MSR3600-28-XS

- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
- In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

MSR3610-XS

- In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2,

Hardware	Default
MSR3620-XS	• and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR3610-I-XS	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR3610-IE-XS	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2. • In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3.
MSR3620-X1-XS	• In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.
MSR3640-XS	• In non-FIPS mode, the SSL server supports TLS

Hardware	Default
MSR3660-XS	1.1, TLS 1.2, and TLS 1.3.
	• In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.
	• In non-FIPS mode, the SSL server supports TLS 1.1, TLS 1.2, and TLS 1.3.
	• In FIPS mode, the SSL server supports TLS 1.1 and TLS 1.2.

Hardware	Default
MSR810-LM-GL	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
MSR810-W-LM-GL	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR830-6EI-GL	• In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
	• In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

Hardware	Default
MSR830-10EI-GL	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR830-6HI-GL	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR830-10HI-GL	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR1004S-5G-GL	- In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
MSR2600-6-X1-GL	In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.

Hardware	Default
MSR3600-28-SI-GL	In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.
	In non-FIPS mode, the SSL server supports SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.
	In FIPS mode, the SSL server supports TLS 1.0, TLS 1.1, and TLS 1.2.

Modified command: version

Use **version** to specify an SSL protocol version for an SSL client policy.

Use **undo version** to restore the default.

Syntax

In non-FIPS mode:

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** }

undo version

In FIPS mode:

version { **tls1.0** | **tls1.1** | **tls1.2** }

undo version

Views

SSL client policy view

Change description

Before modification: An SSL client policy uses SSL protocol version TLS 1.0.

After modification: The default settings vary by device model, as shown in the following tables:

Default

Hardware	Default
MSR610	An SSL client policy uses SSL protocol version TLS 1.1.
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	An SSL client policy uses SSL protocol version TLS 1.0.

Hardware	Default
MSR810-LMS, MSR810-LUS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR810-SI, MSR810-LM-SI	An SSL client policy uses SSL protocol version TLS 1.0.
MSR810-LMS-EA, MSR810-LME	An SSL client policy uses SSL protocol version TLS 1.0.
MSR1004S-5G, MSR1004S-5G-CN	An SSL client policy uses SSL protocol version TLS 1.0.
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	An SSL client policy uses SSL protocol version TLS 1.1.
MSR2600-6-X1, MSR2600-15-X1, MSR2600-15-X1-T	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2600-10-X1	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2630	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28, MSR3600-51	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28-SI, MSR3600-51-SI	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28-G-DP, MSR3600-51-G-DP	An SSL client policy uses SSL protocol version TLS 1.1.
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	An SSL client policy uses SSL protocol version TLS 1.1.

Hardware	Default
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3610-G, MSR3620-G	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3640-G	An SSL client policy uses SSL protocol version TLS 1.1.
MSR3640-X1-HI	An SSL client policy uses SSL protocol version TLS 1.1.

Hardware	Default
MSR810-W-WiNet, MSR810-LM-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-4LM-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2600-6-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2600-10-X1-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2630-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28-WiNet	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3610-X1-WiNet	An SSL client policy uses SSL protocol version TLS 1.1.
MSR3610-WiNet, MSR3620-10-WiNet,	An SSL client policy uses

Hardware	Default
MSR3620-DP-WiNet, MSR3620-WiNet, MSR3660-WiNet	SSL protocol version TLS 1.0.

Hardware	Default
MSR860-6EI-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR860-6HI-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2630-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3610-XS	An SSL client policy uses SSL protocol version TLS 1.1.
MSR3620-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3610-I-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3610-IE-XS	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3620-X1-XS	An SSL client policy uses SSL protocol version TLS 1.1.
MSR3640-XS	An SSL client policy uses SSL protocol version TLS 1.1.
MSR3660-XS	An SSL client policy uses SSL protocol version TLS 1.1.

Hardware	Default
MSR810-LM-GL	An SSL client policy uses SSL protocol version TLS 1.0.

Hardware	Default
MSR810-W-LM-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-6EI-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-10EI-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-6HI-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR830-10HI-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR1004S-5G-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR2600-6-X1-GL	An SSL client policy uses SSL protocol version TLS 1.0.
MSR3600-28-SI-GL	An SSL client policy uses SSL protocol version TLS 1.0.

Modified feature: Disabling SSL session renegotiation

Feature change description

By default, the following devices do not support enabling SSL session renegotiation: MSR610, MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN, MSR3600-28-G-DP, MSR3600-51-G-DP, MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1, MSR3640-G, MSR3640-X1-HI, MSR3610-X1-WiNet, MSR3610-XS, MSR3620-X1-XS, MSR3640-XS, and MSR3660-XS.

Command changes

Modified command: ssl renegotiation disable

Use **ssl renegotiation disable** to disable SSL session renegotiation.

Use **undo ssl renegotiation disable** to restore the default.

Syntax

ssl renegotiation disable

undo ssl renegotiation disable

Views

System view

Change description

Before modification: SSL session renegotiation is enabled.

After modification: The default settings vary by device model, as shown in the following tables:

Default

Hardware	Default
MSR610	SSL session renegotiation is disabled.
MSR810, MSR810-W, MSR810-W-DB, MSR810-LM, MSR810-W-LM, MSR810-10-PoE, MSR810-LM-HK, MSR810-W-LM-HK, MSR810-LM-CNDE-SJK, MSR810-CNDE-SJK, MSR810-EI, MSR810-LM-EA, MSR810-LM-EI	SSL session renegotiation is enabled.
MSR810-LMS, MSR810-LUS	SSL session renegotiation is enabled.
MSR810-SI, MSR810-LM-SI	SSL session renegotiation is enabled.
MSR810-LMS-EA, MSR810-LME	SSL session renegotiation is enabled.
MSR1004S-5G, MSR1004S-5G-CN	SSL session renegotiation is enabled.
MSR1104S-W, MSR1104S-W-CAT6, MSR1104S-5G-CN, MSR1104S-W-5G-CN	SSL session renegotiation is disabled.
MSR2600-6-X1, MSR2600-15-X1-T, MSR2600-15-X1,	SSL session renegotiation is enabled.
MSR2600-10-X1	SSL session renegotiation is enabled.
MSR2630	SSL session renegotiation is enabled.
MSR3600-28, MSR3600-51	SSL session renegotiation is enabled.
MSR3600-28-SI, MSR3600-51-SI	SSL session renegotiation is enabled.

Hardware	Default
MSR3600-28-X1, MSR3600-28-X1-DP, MSR3600-51-X1, MSR3600-51-X1-DP	SSL session renegotiation is enabled.
MSR3600-28-G-DP, MSR3600-51-G-DP	SSL session renegotiation is disabled.
MSR3610-I-DP, MSR3610-IE-DP, MSR3610-IE-ES, MSR3610-IE-EAD, MSR-EAD-AK770, MSR3610-I-IG, MSR3610-IE-IG	SSL session renegotiation is enabled.
MSR3610-X1, MSR3610-X1-DP, MSR3610-X1-DC, MSR3610-X1-DP-DC, MSR3620-X1, MSR3640-X1	SSL session renegotiation is disabled.
MSR3610, MSR3620, MSR3620-DP, MSR3640, MSR3660	SSL session renegotiation is enabled.
MSR3610-G, MSR3620-G	SSL session renegotiation is enabled.
MSR3640-G	SSL session renegotiation is disabled.
MSR3640-X1-HI	SSL session renegotiation is disabled.

Hardware	Default
MSR810-W-WiNet, MSR810-LM-WiNet	SSL session renegotiation is enabled.
MSR830-4LM-WiNet	SSL session renegotiation is enabled.
MSR830-5BEI-WiNet, MSR830-6EI-WiNet, MSR830-10BEI-WiNet	SSL session renegotiation is enabled.
MSR830-6BHI-WiNet, MSR830-10BHI-WiNet	SSL session renegotiation is enabled.
MSR2600-6-WiNet	SSL session renegotiation is enabled.
MSR2600-10-X1-WiNet	SSL session renegotiation is enabled.
MSR2630-WiNet	SSL session renegotiation is enabled.
MSR3600-28-WiNet	SSL session renegotiation is enabled.
MSR3610-X1-WiNet	SSL session renegotiation is disabled.

Hardware	Default
MSR3610-WiNet, MSR3620-DP-WiNet, MSR3660-WiNet	MSR3620-10-WiNet, MSR3620-WiNet, SSL session renegotiation is enabled.

Hardware	Default
MSR860-6EI-XS	SSL session renegotiation is enabled.
MSR860-6HI-XS	SSL session renegotiation is enabled.
MSR2630-XS	SSL session renegotiation is enabled.
MSR3600-28-XS	SSL session renegotiation is enabled.
MSR3610-XS	SSL session renegotiation is disabled.
MSR3620-XS	SSL session renegotiation is enabled.
MSR3610-I-XS	SSL session renegotiation is enabled.
MSR3610-IE-XS	SSL session renegotiation is enabled.
MSR3620-X1-XS	SSL session renegotiation is disabled.
MSR3640-XS	SSL session renegotiation is disabled.
MSR3660-XS	SSL session renegotiation is disabled.

Hardware	Default
MSR810-LM-GL	SSL session renegotiation is enabled.
MSR810-W-LM-GL	SSL session renegotiation is enabled.
MSR830-6EI-GL	SSL session renegotiation is enabled.
MSR830-10EI-GL	SSL session renegotiation is enabled.

Hardware	Default
MSR830-6HI-GL	SSL session renegotiation is enabled.
MSR830-10HI-GL	SSL session renegotiation is enabled.
MSR1004S-5G-GL	SSL session renegotiation is enabled.
MSR2600-6-X1-GL	SSL session renegotiation is enabled.
MSR3600-28-SI-GL	SSL session renegotiation is enabled.

Modified feature: Displaying information about SDWAN IPsec tunnels

Feature change description

As from this release, the device supports displaying the **Path MTU**, **Remote Site**, **Site ID**, **Device ID**, **Interface ID**, and **Link ID** fields in the output for the **display ipsec sdwan-tunnel** command.

Command changes

Modified command: display ipsec sdwan-tunnel

Old syntax

display ipsec sdwan-tunnel [**brief** | **count** | **tunnel-id** *tunnel-id*]

New syntax

display ipsec sdwan-tunnel [**brief** | **count** | **remote-site** *site-id device-id interface-id* | **tunnel-id** *tunnel-id*]

Views

Any view

Change description

The **remote-site** *site-id device-id interface-id* option is added to specify an IPsec tunnel by the remote site ID, device ID, and SDWAN tunnel interface ID. The *site-id* argument represents the site ID, in the range of 1 to 65535. The *device-id* argument represents the device ID, in the range of 1 to 255. The *interface-id* argument represents the interface ID, in the range of 1 to 255.

Before modification: The **Path MTU**, **Remote Site**, **Site ID**, **Device ID**, **Interface ID**, and **Link ID** fields were not displayed in the output for this command.

```
<Sysname> display ipsec sdwan-tunnel
Tunnel ID: 1
```

```
Status: Active
SA's SPI:
    Outbound: 1091054028 (0x410829cc) [ESP]
    Inbound: 2400381837 (0x8f12eb8d) [ESP]
Tunnel:
    Local address: 11.1.2.1
    Remote address: 11.1.3.1
```

After modification: The **Path MTU**, **Remote Site**, **Site ID**, **Device ID**, **Interface ID**, and **Link ID** fields are displayed in the output for this command.

```
<Sysname> display ipsec sdwan-tunnel
Tunnel ID: 1
Status: Active
Path MTU: 1432
SA's SPI:
    Outbound: 1091054028 (0x410829cc) [ESP]
    Inbound: 2400381837 (0x8f12eb8d) [ESP]
Tunnel:
    Local address: 11.1.2.1
    Remote address: 11.1.3.1
Remote Site:
    Site ID: 10
    Device ID: 10
    Interface ID: 35
    Link ID: 1315875 (0x141423)

<Sysname> display ipsec sdwan-tunnel remote-site 10 10 35
Tunnel ID: 1
Status: Active
Path MTU: 1432
SA's SPI:
    Outbound: 1091054028 (0x410829cc) [ESP]
    Inbound: 2400381837 (0x8f12eb8d) [ESP]
Tunnel:
    Local address: 11.1.2.1
    Remote address: 11.1.3.1
Remote Site:
    Site ID: 10
    Device ID: 10
    Interface ID: 35
    Link ID: 1315875 (0x141423)
```

Table 106 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel.
Status	Status of the IPsec tunnel. - In a VSRP scenario, this field displays either Active or Standby. - In standalone mode, this field always displays Active.

Path MTU	Path MTU of the SDWAN IPsec SA.
SA's SPI	SPIs of the inbound and outbound IPsec SAs.
Outbound	Valid outbound SPI in the IPsec tunnel.
Inbound	Valid inbound SPI in the IPsec tunnel.
Tunnel	Addresses of the local and remote ends of the IPsec tunnel.
Local address	Local IP address of the IPsec tunnel.
Remote address	Remote IP address of the IPsec tunnel.
Remote Site	Remote site of the SDWAN IPsec tunnel.
Site ID	ID of the site.
Device ID	ID of the device.
Interface ID	Interface ID of the SDWAN IPsec tunnel interface.
Link ID	Link ID assigned to the TTE. A link ID identifies a TTE connection.

Modified feature: Specifying the user information required for client authentication

Feature change description

As from this release, the device supports specifying the user information required for client authentication.

Command changes

Modified command: client-authentication xauth user

Old syntax

```
client-authentication xauth user username password { cipher | simple } string
undo client-authentication xauth user
```

New syntax

```
client-authentication xauth { aaa-auth-server | user username password { cipher | simple } string }
undo client-authentication xauth { aaa-auth-server | user }
```

Views

IKE profile view

Change description

The syntax for this command has changed from **client-authentication xauth user** to **client-authentication xauth**.

The **aaa-auth-server** keyword is added to obtain the user information required for client authentication from the AAA server.

The default for this command has changed:

- Before modification: The username and password required for client authentication is not specified.
- After modification: The user information required for client authentication is not specified.

The following usage guidelines for this command are added:

Configure this command in the IKE profile used by a branch gateway. The branch gateway can then use the specified user information to perform AAA authentication and establish an IPsec tunnel with the IPsec gateway at the enterprise headquarters.

You can use the following methods to specify the user information required for client authentication:

- **Obtaining the user information from the AAA server**—The client obtains user identity information from the AAA server and then sends it to the peer to perform identity authentication. Use this method when the peer uses the JIT server to perform identity authentication on clients. For more information about AAA, see *Security Configuration Guide*.
- **Manually specifying the user information**—The client sends the specified username and password to the peer to perform identity authentication.

If you execute this command multiple times, the most recent configuration takes effect.

Modified feature: Displaying information about IKE SAs

Feature change description

As from this release, the device supports displaying the **Output interface index** field in the output for the **display ike sa** command.

Command changes

Modified command: display ike sa

Use **display ike sa** to display information about IKE SAs.

Syntax

```
display ike sa [ verbose [ connection-id connection-id | remote-address [ ipv6 ]  
remote-address [ vpn-instance vpn-instance-name ] ] | count ]
```

Views

Any view

Change description

Before modification: The **Output interface index** field was not displayed in the output for this command.

```
<Sysname> display ike sa verbose
```

```

-----
Connection ID: 2
Outside VPN: 1
Inside VPN: 1
Profile: prof1
Transmitting entity: Initiator
Initiator cookie: 1bcf453f0a217259
Responder cookie: 5e32a74dfa66a0a4
-----

Local IP/port: 4.4.4.4/500
Local ID type: IPV4_ADDR
Local ID: 4.4.4.4

Remote IP/port: 4.4.4.5/500
Remote ID type: IPV4_ADDR
Remote ID: 4.4.4.5

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: SHA1
Encryption-algorithm: AES-CBC-128

Life duration(sec): 86400
Remaining key duration(sec): 86379
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected

Extend authentication: Enabled
Assigned IP address: 192.168.2.1
Vendor ID index: 0xald
Vendor ID sequence number: 0x0

```

After modification: The **Output interface index** field is displayed in the output for this command.

<Sysname> display ike sa verbose

```

-----
Connection ID: 2
Outside VPN: 1
Inside VPN: 1
Profile: prof1
Transmitting entity: Initiator
Initiator cookie: 1bcf453f0a217259
Responder cookie: 5e32a74dfa66a0a4
Output interface index: 2
-----

Local IP/port: 4.4.4.4/500
Local ID type: IPV4_ADDR
Local ID: 4.4.4.4

Remote IP/port: 4.4.4.5/500

```

```
Remote ID type: IPV4_ADDR
Remote ID: 4.4.4.5

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: SHA1
Encryption-algorithm: AES-CBC-128

Life duration(sec): 86400
Remaining key duration(sec): 86379
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected

Extend authentication: Enabled
Assigned IP address: 192.168.2.1
Vendor ID index: 0xald
Vendor ID sequence number: 0x0
```

Table 107 Command output

Field	Description
Output interface index	Output interface index for IKE negotiation packets.

Modified feature: Displaying IKE statistics

Feature change description

As from this release, the **display ike statistics** command supports displaying the following fields:

- In packets.
- In dropped packets.
- Out packets.
- Out dropped packets.
- Packets enqueued.
- Packets processed.

Command changes

Modified command: display ike statistics

Use **display ike statistics** to display IKE statistics.

Syntax

display ike statistics

Views

Any view

Change description

Before modification: The **In packets**, **In dropped packets**, **Out packets**, **Out dropped packets**, **Packets enqueued**, **Packets processed** fields were not added to the output for this command.

```
<Sysname> display ike statistics
```

IKE statistics:

```
No matching proposal: 0
Invalid ID information: 0
Unavailable certificate: 0
Unsupported DOI: 0
Unsupported situation: 0
Invalid proposal syntax: 0
Invalid SPI: 0
Invalid protocol ID: 0
Invalid certificate: 0
Authentication failure: 0
Invalid flags: 0
Invalid message id: 0
Invalid cookie: 0
Invalid transform ID: 0
Malformed payload: 0
Invalid key information: 0
Invalid hash information: 0
Unsupported attribute: 0
Unsupported certificate type: 0
Invalid certificate authority: 0
Invalid signature: 0
Unsupported exchange type: 0
No available SA: 1
Retransmit timeout: 0
Not enough memory: 0
Enqueue fails: 0
Failures to send R_U_THERE DPD packets: 0
Failures to receive R_U_THERE DPD packets: 0
Failures to send ACK DPD packets: 0
Failures to receive ACK DPD packets: 0
Sent P1 SA lifetime change packets: 0
Received P1 SA lifetime change packets: total=0, process failures=0 (no SA=0, failures
to reset SA soft lifetime=0, failures to reset SA hard lifetime=0)
Sent P2 SA lifetime change packets: 0
Received P2 SA lifetime change packets: total=0, process failures=0
```

After modification: The **In packets**, **In dropped packets**, **Out packets**, **Out dropped packets**, **Packets enqueued**, **Packets processed** fields are added to the output for this command.

```
<Sysname> display ike statistics
```

IKE statistics:

```
No matching proposal: 0
Invalid ID information: 0
Unavailable certificate: 0
Unsupported DOI: 0
```

```

Unsupported situation: 0
Invalid proposal syntax: 0
Invalid SPI: 0
Invalid protocol ID: 0
Invalid certificate: 0
Authentication failure: 0
Invalid flags: 0
Invalid message id: 0
Invalid cookie: 0
Invalid transform ID: 0
Malformed payload: 0
Invalid key information: 0
Invalid hash information: 0
Unsupported attribute: 0
Unsupported certificate type: 0
Invalid certificate authority: 0
Invalid signature: 0
Unsupported exchange type: 0
No available SA: 1
Retransmit timeout: 0
Not enough memory: 0
Enqueue fails: 0
Failures to send R_U_THERE DPD packets: 0
Failures to receive R_U_THERE DPD packets: 0
Failures to send ACK DPD packets: 0
Failures to receive ACK DPD packets: 0
Sent P1 SA lifetime change packets: 0
Received P1 SA lifetime change packets: total=0, process failures=0 (no SA=0, failures
to reset SA soft lifetime=0, failures to reset SA hard lifetime=0)
Sent P2 SA lifetime change packets: 0
Received P2 SA lifetime change packets: total=0, process failures=0
In packets: 0
In dropped packets: 0
Out packets: 0
Out dropped packets: 0
Packets enqueued: 0
Packets processed: 0

```

Table 108 Command output

Field	Description
In packets	Total number of received IKE packets, including IKEv1 and IKEv2 packets (because the packets have not been parsed).
In dropped packets	Total number of dropped packets in packet reception.
Out packets	Total number of sent packets.
Out dropped packets	Total number of dropped packets in packet sending.
Packets enqueued	Total number of packets waiting to be processed.
Packets processed	Total number of processed packets.

Modified feature: Displaying the IKEv2 SA information

Feature change description

As from this release, the **display ikev2 sa count** command supports displaying the total number of IKEv2 SAs with the **Total SAs** field and displaying the number of negotiating IKEv2 SAs with the **Negotiating SAs** field.

Command changes

Modified command: display ikev2 sa

Use **display ikev2 sa** to display the IKEv2 SA information.

Syntax

```
display ikev2 sa [ count | [ { local | remote } { ipv4-address | ipv6 ipv6-address }  
[ vpn-instance vpn-instance-name ] ] [ verbose [ tunnel tunnel-id ] ] ]
```

Views

Any view

Change description

Before modification: The **display ikev2 sa count** command supports displaying the total number of IKEv2 SAs with the **IKEv2 SAs count** field.

```
[Sysname] display ikev2 sa count  
IKEv2 SAs count: 0
```

After modification: The **display ikev2 sa count** command supports displaying the total number of IKEv2 SAs with the **Total SAs** field and displaying the number of negotiating IKEv2 SAs with the **Negotiating SAs** field.

```
[Sysname] display ikev2 sa count  
Total SAs: 10  
Negotiating SAs: 4
```

Modified feature: Displaying IKEv2 statistics

Feature change description

As from this release, the **display ikev2 statistics** command supports displaying the following fields:

- Wait auth timeouts.
- Packets enqueued.
- Packets processed.

- Out packets.
- Out dropped packets.
- Messages in current queue.

Command changes

Modified command: display ikev2 statistics

Use **display ikev2 statistics** to display IKEv2 statistics.

Syntax

display ikev2 statistics

Views

Any view

Change description

Before modification: The **Wait auth timeouts**, **Packets enqueued**, **Packets processed**, **Out packets**, **Out dropped packets**, **Messages in current queue** fields were not added to the output for this command.

```
<Sysname> display ikev2 statistics
```

```
IKEv2 statistics:
```

```
Unsupported critical payload: 0
Invalid IKE SPI: 0
Invalid major version: 0
Invalid syntax: 0
Invalid message ID: 0
Invalid SPI: 0
No proposal chosen: 0
Invalid KE payload: 0
Authentication failed: 0
Single pair required: 0
TS unacceptable: 0
Invalid selectors: 0
Temporary failure: 0
No child SA: 0
Unknown other notify: 0
No enough resource: 0
Enqueue error: 0
No IKEv2 SA: 0
Packet error: 0
Other error: 0
Retransmit timeout: 0
DPD detect error: 0
Del child for IPsec message: 1
Del child for deleting IKEv2 SA: 1
Del child for receiving delete message: 0
```


Before modification: The **Wait auth timeouts**, **Packets enqueued**, **Packets processed**, **Out packets**, **Out dropped packets**, **Messages in current queue** fields are added to the output for this command.

```
<Sysname> display ikev2 statistics
IKEv2 statistics:
  Unsupported critical payload: 0
  Invalid IKE SPI: 0
  Invalid major version: 0
  Invalid syntax: 0
  Invalid message ID: 0
  Invalid SPI: 0
  No proposal chosen: 0
  Invalid KE payload: 0
  Authentication failed: 0
  Single pair required: 0
  TS unacceptable: 0
  Invalid selectors: 0
  Temporary failure: 0
  No child SA: 0
  Unknown other notify: 0
  No enough resource: 0
  Enqueue error: 0
  No IKEv2 SA: 0
  Packet error: 0
  Other error: 0
  Retransmit timeout: 0
  DPD detect error: 0
  Del child for IPsec message: 1
  Del child for deleting IKEv2 SA: 1
  Del child for receiving delete message: 0
  Wait auth timeouts: 0
  Packets enqueued: 0
  Packets processed: 0
  Out packets: 0
  Out dropped packets: 0
  Messages in current queue: 0
```

Table 109 Command output

Field	Description
Wait auth timeouts	Total count of timeouts for packets waiting for authentication.
Packets enqueued	Total number of packets waiting to be processed.
Packets processed	Total number of processed packets.
Out packets	Total number of sent packets.
Out dropped packets	Total number of dropped packets in packet sending.
Messages in current queue	Total number of messages waiting to be processed in the current queue.

Modified feature: Support for the incremental increase in user locking period

Feature change description

The locking period of an account will increment each time the account fails the maximum number of login attempts again after the locking timer expires.

Command changes

Modified command: password-control login-attempt

Old syntax

```
password-control login-attempt login-times [ exceed { lock | lock-time time | unlock } ]  
undo password-control login-attempt
```

New syntax

```
password-control login-attempt login-times [ exceed { lock | lock-time time  
[ autoincrement max-lock-time ] | unlock } ]  
undo password-control login-attempt
```

Views

System view
User group view
Local user view

Change description

The **autoincrement** *max-lock-time* option is added.

autoincrement *max-lock-time*: Enables the locking period of an account to increment each time the account fails the maximum number of login attempts again after the locking timer expires. The *max-lock-time* argument represents the maximum locking period, in the range of 100 to 360 in minutes, and must be equal to or greater than the value for the **lock-time** *time* option. For example, if the *time* argument is *x* and the *max-lock-time* argument is *y*, the account is locked for *x* minutes when the account fails the maximum number of login attempts for the first time. When the account fails the maximum number of login attempts for the *n*th time, the account is locked for *n***x* minutes. If the product of *n***x* is greater than *y*, the account is locked only for *y* minutes, and the locking period will not increment for subsequent login failures.

Release 6728P25

None.

Release 6728P20

None.

Release 6728P15

None.

Release 0821P11

None.

Release 0809P33

None.

Release 0809P32

None.

Release 0809P29

This version has the following changes:

[Modified feature: Configuring an IPv6 static route](#)

Modified feature: Configuring an IPv6 static route

Feature change description

As from this version, you can associate an IPv6 static route with a track entry to detect the reachability of the route's next hop.

Command changes

Modified command: ipv6 route-static

Old syntax

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number  
[ next-hop-address ] [ bfd { control-packet | echo-packet } [ bfd-source ipv6-address ] |  
permanent ] | [ vpn-instance d-vpn-instance-name ] next-hop-address [ bfd  
control-packet bfd-source ipv6-address | permanent ] } [ preference preference ] [ tag  
tag-value ] [ description text ]
```

```
undo ipv6 route-static ipv6-address prefix-length [ interface-type interface-number  
[ next-hop-address ] | [ vpn-instance d-vpn-instance-name ] next-hop-address ]  
[ preference preference ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length  
{ interface-type interface-number [ next-hop-address ] [ bfd { control-packet |  
echo-packet } [ bfd-source ipv6-address ] | permanent ] | next-hop-address [ public ]  
[ bfd control-packet bfd-source ipv6-address | permanent ] | vpn-instance  
d-vpn-instance-name next-hop-address [ bfd control-packet bfd-source ipv6-address |  
permanent ] } [ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length  
[ interface-type interface-number [ next-hop-address ] | next-hop-address [ public ] |  
vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference ]
```

New syntax

```
ipv6 route-static ipv6-address prefix-length { interface-type interface-number  
[ next-hop-address ] [ bfd { control-packet | echo-packet } [ bfd-source ipv6-address ] |  
permanent | track track-entry-number ] | [ vpn-instance d-vpn-instance-name ]  
next-hop-address [ bfd control-packet bfd-source ipv6-address | permanent | track  
track-entry-number ] } [ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ipv6 route-static ipv6-address prefix-length [ interface-type interface-number  
[ next-hop-address ] | [ vpn-instance d-vpn-instance-name ] next-hop-address ]  
[ preference preference ]
```

```
ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length  
{ interface-type interface-number [ next-hop-address ] [ bfd { control-packet |  
echo-packet } [ bfd-source ipv6-address ] | permanent | track track-entry-number ] |  
next-hop-address [ public ] [ bfd control-packet bfd-source ipv6-address | permanent |  
track track-entry-number ] | vpn-instance d-vpn-instance-name next-hop-address [ bfd  
control-packet bfd-source ipv6-address | permanent | track track-entry-number ] }  
[ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address prefix-length  
[ interface-type interface-number [ next-hop-address ] | next-hop-address [ public ] |  
vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference ]
```

Views

System view

Change description

The **track track-entry-number** option was added. This option associates the IPv6 static route with a track entry. The *track-entry-number* argument represents the track entry number in the range of 1 to 1024.

Release 0809P27

This release has the following changes:

- New feature: Configuring the DHCP-designated default router as the next hop of a static route
- New feature: Source IP pools for outgoing packets sent by an HTTP proxy service
- Modified feature: Displaying HTTP proxy configuration information

New feature: Configuring the DHCP-designated default router as the next hop of a static route

Configuring the DHCP-designated default router as the next hop of a static route

About this task

After an interface obtains an IP address and gateway address through DHCP, the device automatically generates a static route with the interface as the output interface. The destination address of the static route is 0.0.0.0/0 and the next hop of the static route is the default router (the gateway address designated by the DHCP server). This static route cannot form ECMP routes with manually configured static routes. The device uses this static route to guide traffic forwarding only after the manually configured static routes become invalid.

Perform this task to use both the automatically generated static route and the manually configured static routes to guide traffic forwarding. The task is applicable when the device has dual egress WAN links.

This task enables the device to automatically generate a static route destined for the specified network with the DHCP-designated default router as the next hop. This static route takes effect only after the output interface obtains an IP address and gateway address through DHCP, and becomes invalid upon the DHCP lease expiration. The next hop of this static route changes as the gateway address of the output interface changes. In addition, this static route cannot form ECMP routes with manually configured static routes.

Restrictions and guidelines

When you configure the next hop of a static route as the DHCP-designated default router, make sure the output interface of the static route is a broadcast interface.

Procedure

1. Enter system view.
system-view

2. Configure a static route and specify the default router designated by the DHCP server for the output interface as the next hop of the static route.

Public network:

```
ip route-static { dest-address { mask-length | mask } | group group-name } interface-type interface-number dhcp [ backup-interface interface-type interface-number ] [ backup-nexthop backup-nexthop-address ] [ permanent ] | permanent | track track-entry-number ] [ preference preference ] [ tag tag-value ] [ description text ]
```

VPN:

```
ip route-static vpn-instance s-vpn-instance-name dest-address { mask-length | mask } interface-type interface-number dhcp [ backup-interface interface-type interface-number ] [ backup-nexthop backup-nexthop-address ] [ permanent ] | permanent | track track-entry-number ] [ preference preference ] [ tag tag-value ] [ description text ]
```

```
ip route-static vpn-instance s-vpn-instance-name group group-name interface-type interface-number dhcp [ backup-interface interface-type interface-number ] [ backup-nexthop backup-nexthop-address ] [ permanent ] ] [ preference preference ] [ tag tag-value ] [ description text ]
```

By default, no static route is configured with the DHCP-designated default router as the next hop.

Command reference

Modified command: ip route-static

Old syntax

```
ip route-static { dest-address { mask-length | mask } | group group-name } interface-type interface-number [ next-hop-address ] [ backup-interface interface-type interface-number ] [ backup-nexthop backup-nexthop-address ] [ permanent ] | bfd { control-packet | echo-packet } | permanent | track track-entry-number ] [ ldp-sync ] [ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ip route-static { dest-address { mask-length | mask } | group group-name } [ interface-type interface-number [ next-hop-address ] | next-hop-address | vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference ]
```

New syntax

```
ip route-static { dest-address { mask-length | mask } | group group-name } interface-type interface-number [ dhcp | next-hop-address ] [ backup-interface interface-type interface-number ] [ backup-nexthop backup-nexthop-address ] [ permanent ] | bfd { control-packet | echo-packet } | permanent | track track-entry-number ] [ ldp-sync ] [ preference preference ] [ tag tag-value ] [ description text ]
```

```
undo ip route-static { dest-address { mask-length | mask } | group group-name } [ interface-type interface-number [ dhcp | next-hop-address ] | next-hop-address | vpn-instance d-vpn-instance-name next-hop-address ] [ preference preference ]
```

Views

System view

Change description

The **dhcp** keyword was added. This keyword specifies the default router designated by the DHCP server for the output interface as the next hop of the static route.

New feature: Source IP pools for outgoing packets sent by an HTTP proxy service

Configuring source IP pools for outgoing packets sent by an HTTP proxy service

About this task

By default, an HTTP proxy service uses the IP address of the outbound interface as the source IP address for packets forwarded to Web servers. An IP address supports a maximum of 65535 TCP connections.

This feature allows an HTTP proxy service to establish more TCP connections to Web servers. After you specify a source IP pool for an HTTP proxy service, the HTTP proxy service will use IP addresses in the source IP pools as the source IP addresses of outgoing packets.

Restrictions and guidelines

You can repeat this command to configure a maximum of 32 source IP pools. The IP address ranges of all source IP pools cannot overlap with each other. Make sure the IP pools configured for the same HTTP proxy service belong to the same VPN instance and that configured for different HTTP proxy services belong to different VPN instances.

Procedure

1. Enter system view.

system-view

2. Create an HTTP proxy service and enter its view.

http-proxy service *service-name*

3. Configure a source IP pool for outgoing packets sent by the HTTP proxy service.

ip-pool *start-address end-address* [**vpn-instance** *vpn-instance-name*]

By default, no source IP pools are configured for outgoing packets sent by the HTTP proxy service.

Command reference

ip-pool

Use **ip-pool** to configure a source IP pool for outgoing packets sent by an HTTP proxy service.

Use **undo ip-pool** to delete a source IP pool for outgoing packets sent by an HTTP proxy service.

Syntax

ip-pool *start-address end-address* [**vpn-instance** *vpn-instance-name*]

undo ip-pool [*start-address end-address* [**vpn-instance** *vpn-instance-name*]]

Default

No source IP pools are configured for outgoing packets sent by an HTTP proxy service.

Views

HTTP proxy service view

Predefined user roles

network-admin

mdc-admin

Parameters

start-address end-address: Specifies the start and end IP addresses of a source IP pool. The end IP address cannot be lower than the start IP address.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the IP pool belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the IP pool does not belong to any VPN instance, do not specify this option.

Usage guidelines

By default, an HTTP proxy service uses the IP address of the outbound interface as the source IP address for packets forwarded to Web servers. An IP address supports a maximum of 65535 TCP connections.

To allow more TCP connections to be established between an HTTP proxy service and Web servers, use this command to configure a source IP pool. The HTTP proxy service will use IP addresses in the source IP pools as the source IP addresses of outgoing packets.

You can repeat this command to configure a maximum of 32 source IP pools. The IP address ranges of all source IP pools cannot overlap with each other. Make sure the IP pools configured for the same HTTP proxy service belong to the same VPN instance and that configured for different HTTP proxy services belong to different VPN instances.

Examples

```
# Configure a source IP pool for outgoing packets sent by HTTP proxy service test.
<Sysname> system-view
[Sysname] http-proxy service test
[Sysname-http-proxy-service-test] ip-pool 1.1.1.1 1.1.1.100 vpn-instance vpn1
```

Modified feature: Displaying HTTP proxy configuration information

Feature change description

From this release, source IP pool configuration was added to HTTP proxy configuration information displayed by the **display http-proxy** command.

Command changes

Modified command: display http-proxy

Syntax

```
display http-proxy { server-group [ group-name ] | service [ service-name ] }
```

Views

Any view

Change description

The source IP pool configuration information was added to the command output:

```
IP pools:                1.1.1.1 to 1.1.1.2 vpn1
                        2.2.2.1 to 2.2.3.1 vpn1
```

Table 110 Command output

Field	Description
IP pools	Source IP pools used by the HTTP proxy service to send packets to Web servers. This field displays N/A if no IP pools are configured.

Release 0707P24

This release has the following changes:

Modified feature: [Processing for user IP conflicts on an LNS](#)

Modified feature: [Login password control](#)

Modified feature: Processing for user IP conflicts on an LNS

Feature change description

When the IP address of an L2TP user that newly comes online conflicts with the IP address of an online L2TP user, you can select to forbid the new user from coming online or forcibly log out the existing user.

Command changes

New command: l2tp user-ip-conflict offline

For more information about this command, see *H3C MSR810[2600][3600] Routers Command References (V7)*.

Modified feature: Login password control

Feature change description

From this release, strong password requirements are enforced on login passwords to enhance device security.

Command changes

Modified commands:

- **set authentication password**
- **display password-control**
- **password-control { aging | composition | history | length } enable**
- **password-control complexity**
- **password-control length**
- **password-control super length**

New commands:

- **password-control change-password weak-password enable**
- **local-server log change-password-prompt**

For more information about the commands, see *H3C MSR810 2600 3600 Routers Command References(V7)*.

Release 0707P21

None.

Release 0707P19

None.

Release 0707P16

This release has the following changes:

[Modified feature: Ethernet interface](#)

Modified feature: Ethernet interface

Feature change description

New fields were added to the **display interface** command output.

Command changes

Modified command: display interface

Syntax

display interface [*interface-type* [*interface-number* | *interface-number.subnumber*]] [**brief** [**description** | **down**]]

Views

Any view

Parameters

interface-type: Specifies an interface type.

interface-number: Specifies an interface number.

interface-number.subnumber: Specifies a subinterface number. The *interface-number* argument is an interface number. The *subnumber* argument is the number of a subinterface created under the interface. The value range for the *subnumber* argument is 1 to 4094.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

description: Displays complete interface descriptions. If you do not specify this keyword, the command displays only the first 27 characters of each interface description.

down: Displays information about interfaces in down state and the causes. If you do not specify this keyword, the command displays information about interfaces in all states.

Change description

The following fields were added to the **display interface** command output.

Table 31 Command output

Field	Description
Current system time	Current system time in the YYYY/MM/DD HH:MM:SS format. If the time zone is configured, this field is in the YYYY/MM/DD HH:MM:SS UTC±HH:MM:SS format.
Last time when physical state changed to up	Last time when physical state of the interface changed to up. A hyphen (-) indicates that the physical state of the interface has not changed to up.
Last time when physical state changed to down	Last time when physical state of the interface changed to down. A hyphen (-) indicates that the physical state of the interface has not changed to down.
Peak input rate	Peak rate of inbound traffic in Bps, and the time when the peak inbound traffic rate occurred.
Peak output rate	Peak rate of outbound traffic in Bps, and the time when the peak outbound traffic rate occurred.

Release 0707P12

This release has the following changes:

New feature: RADIUS ACL assignment by ACL name

New feature: RADIUS ACL assignment by ACL name

Support for assigning ACLs by ACL name was added to RADIUS, and the names of authorization ACLs are displayed in the information about AAA users.

Release 0615P16

This release has the following changes:

New feature: mGRE

New feature: Public key management support for Suite B

New feature: PKI support for Suite B

New feature: IPsec support for Suite B

New feature: SSL support for Suite B

New feature: FIPS support for Suite B

New feature: SSH support for Suite B

New feature: EVPN

New feature: SM2 key pair creation

New feature: Built-in AC

New feature: mGRE

Overview

Multipoint Generic Routing Encapsulation (mGRE) is a dynamic VPN technology that uses the Next Hop Resolution Protocol (NHRP).

Traditional GRE tunnels for a VPN are static and require manual configuration and maintenance, resulting in poor extensibility. If branches of an enterprise access the public network by using dynamic IP addresses, it is difficult to set GRE tunnels between the branches.

mGRE can dynamically establish tunnels for the branches, because NHRP can map the private IP address of a branch to its public IP address.

mGRE operation scheme

An mGRE network uses the client/server model. It has the following types of nodes:

- **NHS**—NHRP server, the hub device in the mGRE network. The NHS is the routing information exchange center. It is also the data forwarding center in a NHS-NHC network.
- **NHC**—NHRP client, a spoke device in the mGRE network. Typically, it is the gateway of a branch network. An NHC does not forward data received from other mGRE nodes.

mGRE obtains dynamic public addresses of NHCs through their private addresses to establish mGRE tunnels and forward packets. The public address is the IP address of the interface connected to the Internet. The private address is the IP address of the mGRE tunnel interface.

An NHC registers its public and private addresses with the NHS and it registers its public address whenever the public address changes. An NHC obtains the current public address of a peer NHC from the NHS through NHRP, so the two NHCs can establish an mGRE tunnel over the Internet.

mGRE operation procedure

The mGRE operation includes the following phases:

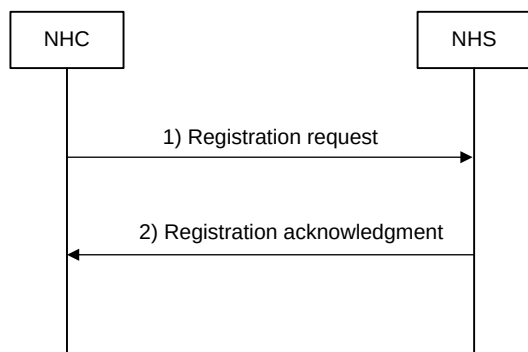
- Registration.
- Tunnel establishment.
- Route learning and packet forwarding.

Registration

As shown in [Figure 10](#), the registration process is as follows:

1. The NHC sends a registration request to the NHS.
2. After the NHS receives the request, it performs the NHRP packet authentication key and GRE key matching. If both keys are matched, registration succeeds. The NHS sends a registration success message to the NHC.

Figure 10 Registration process

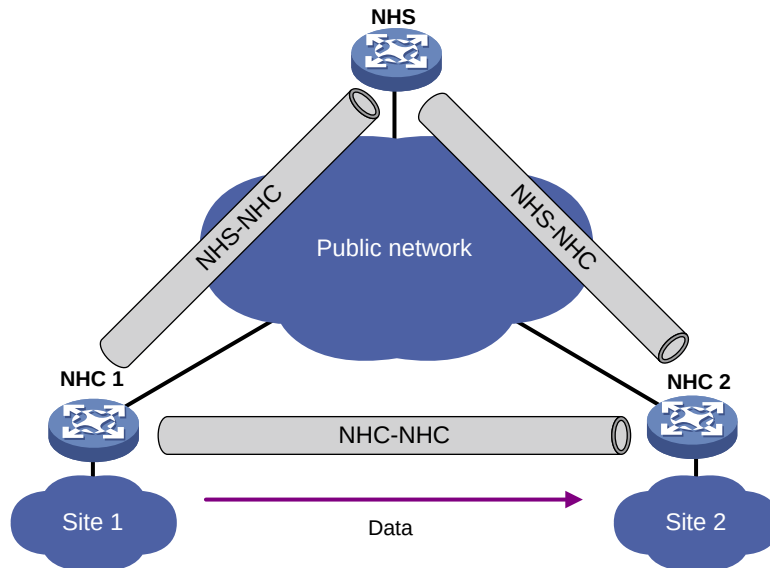


Tunnel establishment

mGRE networks support the following types of networking:

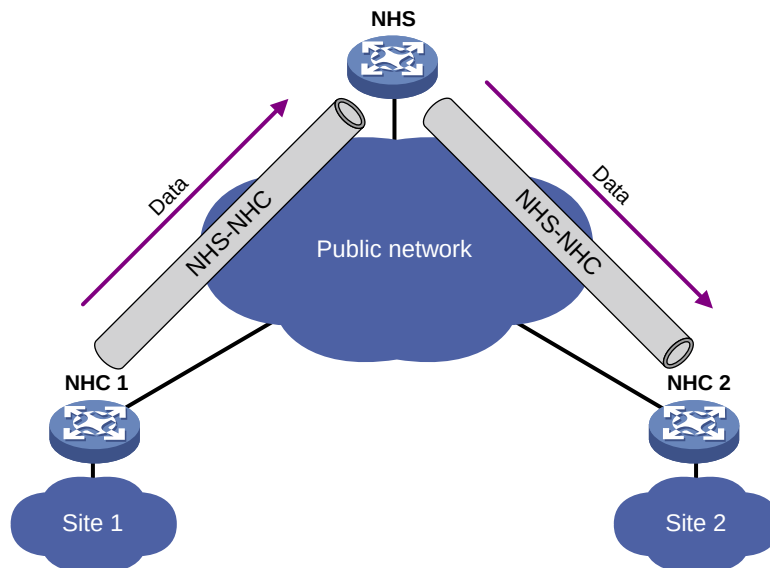
- **Full-mesh network**—NHCs can establish tunnels between each other for direct communication. The NHS acts as the routing information exchange center.

Figure 72 Full-mesh network



- **NHS-NHC network**—NHCs cannot establish tunnels between each other. Instead, they establish tunnels with the NHS. The NHS forwards data for the NHCs. The NHS acts as both the routing information exchange center and the data forwarding center.

Figure 73 NHS-NHC network



A mGRE tunnel is as established as follows:

- **NHC-NHS tunnel establishment process:**
An NHC-NHS tunnel is established in the registration process. During registration, the NHC-NHS tunnel is in initialization state. After registration succeeds, the NHC-NHS tunnel is in success state.
An NHC-NHS tunnel is permanent. An NHC can establish permanent tunnels to any number of NHSs.
- **NHC-NHC tunnel establishment process:**
 - a. In a full-mesh network, when an NHC receives a data packet but finds no tunnel for forwarding the packet, the NHC (initiator) sends an address resolution request to the NHS.

- b. After receiving the request, the NHS looks up the local NHRP mapping table to find the peer NHC (responder) and forwards the request to the peer NHC.
- c. After receiving the request, the peer NHC creates a temporary tunnel and sends an address resolution response to the initiator.

An NHC-NHC tunnel is dynamic. If no data is exchanged within the NHC-NHC tunnel idle timeout, the tunnel will be deleted.

Route learning and packet forwarding

mGRE nodes learn private routes by using dynamic routing protocols.

Dynamic routing must be configured for all private networks and mGRE tunnel interfaces to ensure IP connectivity among the private networks. From the perspective of private networks, an mGRE tunnel is a link that connects different private networks. A dynamic routing protocol discovers neighbors and updates routes over mGRE tunnels, and establishes a routing table.

When an NHC receives a packet destined for a remote private network, it performs the following operations:

1. Searches the routing table for the next hop address to the target private network.
2. Looks up the local NHRP mapping table to obtain the public address that corresponds to the next hop address.
3. Uses the public address as the tunnel destination address to encapsulate the packet.
4. Sends the encapsulated packet to the peer NHC over the mGRE tunnel.

mGRE support for NAT traversal

An NHC-NHC tunnel can traverse a NAT gateway. The tunnel can be established when the tunnel initiator, receiver, or both ends reside behind the NAT gateway.

mGRE configuration task list

To set up an mGRE network, first configure the NHSs and then the NHCs.

ⓘ **IMPORTANT:**

The device can act only as an NHC. It cannot act as an NHS.

To configure mGRE on an NHC:

Tasks at a glance
(Required.) Configuring an mGRE tunnel
(Required.) Configuring routing
(Optional.) Configuring IPsec for an mGRE tunnel

Configuring an mGRE tunnel

The public address of an NHC can be statically configured or dynamically assigned. The private address of an NHC must be statically configured.

To configure an mGRE tunnel:

Step	Command	Remarks
3. Enter system view.	system-view	N/A
4. Create an mGRE tunnel interface and enter tunnel interface view.	interface tunnel <i>number</i> mode mgre	By default, no tunnel interfaces exist.
5. Configure a private address for the tunnel interface.	ip address <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [sub]	By default, no private address is configured for a tunnel interface.
6. Configure a source address or source interface for the tunnel interface.	source { <i>ip-address</i> <i>interface-type</i> <i>interface-number</i> }	By default, no source address or source interface is configured for a tunnel interface. If you specify a source address, it is used as the source IP address of tunneled packets. If you specify a source interface, the primary IP address of this interface is used as the source IP address of tunneled packets.
7. Configure an NHRP packet authentication key.	nhrp authentication [cipher simple] <i>string</i>	By default, no NHRP packet authentication key is configured. NHRP nodes do not authenticate NHRP packets received from each other.
8. Configure an NHRP network ID for the mGRE tunnel.	nhrp network-id <i>number</i>	By default, an mGRE tunnel does not have an NHRP network ID.
9. Configure the holdtime for NHRP mapping entries.	nhrp holdtime <i>seconds</i>	By default, the holdtime of NHRP mapping entries is 7200 seconds.
10. Configure an NHS private-to-public address mapping.	nhrp nhs <i>nhs-address</i> nbma <i>nbma-address</i>	By default, no NHS private-to-public address mappings are configured.
11. (Optional.) Configure a GRE key for the tunnel interface.	gre key <i>key</i>	By default, no GRE key is configured for an mGRE tunnel interface. You must configure the same GRE key or configure no key on both ends of a tunnel. On the device, you must configure different GRE keys for mGRE tunnel interfaces that have the same source address or source interface.
12. (Optional.) Set the DF bit for tunneled packets.	tunnel dfbit enable	By default, the DF bit is not set. Tunneled packets can be fragmented for forwarding.

Configuring routing

mGRE clients support dynamic routing protocols of OSPF, RIP, and BGP.

When you configure routing for an mGRE client, following these restrictions and guidelines:

- When OSPF is used, specify the OSPF interface network type as **broadcast** in a full-mesh network and as **p2mp** in a NHS-NHC network.
- Full-mesh networks do not support RIP. NHS-NHC networks must use the RIP-2 multicast mode and disable the split horizon feature for NHS nodes.

- When BGP is used, configure routing policies to ensure the following:
 - In a full-mesh network, ensure that the local NHC learns a route to the remote private network, and the route's next hop address is the address of the remote NHC.
 - In an NHS-NHC network, ensure that the local NHC learns a route to the remote private network, and the route's next hop address is the address of the NHS.

Configuring IPsec for an mGRE tunnel

The device supports protecting mGRE tunnel data and control packets by using IPsec profiles.

To configure IPsec for an mGRE tunnel:

1. Configure an IPsec transform set to specify the security protocol, authentication and encryption algorithms, and encapsulation type.
2. Configure an IKE-based IPsec profile.
3. Apply the IKE-based IPsec profile to the mGRE tunnel interface.

Displaying and maintaining mGRE

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display information about NHRP mapping entries.	display nhrp map [interface tunnel <i>interface-number</i> [peer <i>ipv4-address</i>]] [verbose]
Display NHRP packet statistics for tunnel interfaces.	display nhrp statistics [interface tunnel <i>interface-number</i>]
Display mGRE session information.	display mgre session [interface tunnel <i>interface-number</i> [peer <i>ipv4-address</i>]] [verbose]
Clear NHRP packet statistics for tunnel interfaces.	reset nhrp statistics [interface tunnel <i>interface-number</i>]
Reset mGRE sessions.	reset mgre session [interface tunnel <i>interface-number</i> [peer <i>ipv4-address</i>]]
Clear mGRE session statistics.	reset mgre statistics [interface tunnel <i>interface-number</i> [peer <i>ipv4-address</i>]]

Command reference

New command: display mgre session

Use **display mgre session** to display mGRE session information.

Syntax

display mgre session [**interface tunnel** *interface-number* [**peer** *ipv4-address*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface tunnel *interface-number*: Specifies an mGRE tunnel interface by its number in the range of 0 to 4095. If you do not specify this option, the command displays mGRE session information for all mGRE tunnel interfaces.

peer *ipv4-address*: Specifies a peer public address. If you do not specify this option, the command displays all mGRE session information for the specified mGRE tunnel interface.

verbose: Displays detailed information about IPv4 mGRE sessions. If you do not specify this keyword, the command displays brief information about mGRE sessions.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all mGRE sessions on all tunnel interfaces.

Examples

Display brief information about all mGRE sessions.

```
<Sysname> display mgre session
Interface          : Tunnell
Number of sessions: 2
Peer NBMA address  Peer protocol address  Type   State        State duration
10.0.0.3           192.168.180.136         C-S    Succeeded    00:30:01
10.0.1.4           192.168.180.137         C-C    Establishing  00:30:02
```

Display brief information about mGRE sessions on the specified tunnel interface.

```
<Sysname> display mgre session interface tunnel 1
Interface          : Tunnell
Number of sessions: 2
Peer NBMA address  Peer protocol address  Type   State        State duration
10.0.0.3           192.168.180.136         C-S    Succeeded    00:30:01
10.0.1.4           192.168.180.137         C-C    Establishing  00:30:02
```

Display brief information about the mGRE session with the specified peer address.

```
<Sysname> display mgre session interface tunnel 1 peer 10.0.0.3
Interface          : Tunnell
Number of sessions: 1
Peer NBMA address  Peer protocol address  Type   State        State duration
10.0.0.3           192.168.180.136         C-S    Succeeded    00:30:01
```

Table 1 Command output

Field	Description
Interface	Name of the mGRE tunnel interface.
Number of sessions	Total number of mGRE sessions on the tunnel interface.
Peer NBMA address	Public address of the peer.
Peer protocol address	IP address of the peer tunnel interface.
Type	mGRE session type: • C-S—The local end is an NHC, and the peer end is the NHS. • C-C—The local end is an NHC, and the peer end is an NHC. • UNKNOWN—The local end is an NHC, and the

Field	Description
	peer end type is unknown.
State	mGRE session state: • Succeeded. • Establishing.
State duration	Duration of the current session state, in the format of hh:mm:ss.

Display detailed information about all IPv4 mGRE sessions.

```
<Sysname> display mgre session verbose
Interface          : Tunnel1
Link protocol      : GRE
Number of sessions: 2
  Peer NBMA address   : 10.0.1.3
  Peer protocol address: 192.168.180.136
  Session type        : C-S
  State               : Succeeded
  State duration      : 00:30:01
  Input : 2201 packets, 218 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
          2163 multicasts, 0 errors

  Peer NBMA address   : 10.0.1.4
  Peer protocol address: 192.168.180.137
  Session type        : C-S
  State               : Succeeded
  State duration      : 00:31:01
  Input : 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors
  Output: 16 packets, 0 data packets, 16 control packets
          0 multicasts, 0 errors

Interface          : Tunnel2
Link protocol      : IPsec-GRE
SA's SPI          :
  Inbound : 187199087 (0xb286e6f) [ESP]
  Outbound: 3562274487 (0xd453feb7) [ESP]
Number of sessions: 1
  Peer NBMA address   : 20.0.0.3
  Peer protocol Aaddress: 192.168.181.137
  Behind NAT          : No
  Session type        : C-C
  SA's SPI            :
    Inbound : 187199087 (0xb286e6f) [ESP]
    Outbound: 3562274487 (0xd453feb7) [ESP]
  State               : Establishing
  State duration      : 00:31:01
```

```

Input : 0 packets, 0 data packets, 0 control packets
        0 multicasts, 0 errors
Output: 1 packets, 0 data packets, 1 control packets
        0 multicasts, 0 errors

```

Display detailed information about IPv4 mGRE sessions on interface **Tunnel1**.

```

<Sysname> display mgre session interface tunnel 1 verbose
Interface          : Tunnel1
Link protocol      : GRE
Number of sessions: 1
  Peer NBMA address : 20.0.0.3
  Peer protocol address: 192.168.181.137
  Behind NAT        : No
  Session type      : C-C
  State             : Succeeded
  State duration    : 00:31:01
  Input : 0 packets, 0 data packets, 0 control packets
          0 multicasts, 0 errors
  Output: 1 packets, 0 data packets, 1 control packets
          0 multicasts, 0 errors

```

Display detailed information about the mGRE session with the peer public address 202.12.12.12.

```

<Sysname> display mgre session peer 202.12.12.12 verbose
Interface          : Tunnel1
Link protocol      : GRE
Number of sessions: 1
  Peer NBMA address : 202.12.12.12
  Peer protocol address: 192.168.180.136
  Session type      : C-S
  State             : Succeeded
  State duration    : 00:30:01
  Input : 2201 packets, 218 data packets, 3 control packets
          2191 multicasts, 0 errors
  Output: 2169 packets, 2168 data packets, 1 control packets
          2163 multicasts, 0 errors

```

Table 2 Command output

Field	Description
Interface	Name of the mGRE tunnel interface.
Link protocol	Encapsulation protocol used by the mGRE tunnel: - GRE. - IPsec-GRE.
Number of sessions	Total number of mGRE sessions on the tunnel interface.
Peer NBMA address	Public address of the peer.
Peer protocol address	IP address of the peer tunnel interface.
SA's SPI	SPI of the inbound and outbound SAs. This field is available when the mGRE tunnel is carried over IPsec.
Behind NAT	Whether the peer NHC has traversed a NAT device.

Field	Description
Session type	mGRE session type: • C-S—The local end is an NHC, and the peer end is the NHS. • C-C—The local end is an NHC, and the peer end is an NHC.
State	mGRE session state: • Succeeded. • Establishing.
State duration	Duration of the current session state, in the format of hh:mm:ss.
Input	Statistics on received packets: • packets—Total number of packets. • data packets—Number of data packets. • control packets—Number of control packets. • multicasts—Number of multicast packets. • errors—Number of error packets.
Output	Statistics on received packets: • packets—Total number of packets. • data packets—Number of data packets. • control packets—Number of control packets. • multicasts—Number of multicast packets. • errors—Number of error packets.

New command: display nhrp map

Use **display nhrp map** to display information about NHRP mapping entries.

Syntax

display nhrp map [**interface tunnel** *interface-number* [**peer** *ipv4-address*]] [**verbose**]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface tunnel *interface-number*: Specifies an mGRE tunnel interface by its number in the range of 0 to 4095. If you do not specify this option, the command displays NHRP mapping table information for all mGRE tunnel interfaces.

peer *ipv4-address*: Specifies a peer public address. If you do not specify this option, the command displays NHRP mapping entries for all peers.

verbose: Displays detailed information about NHRP mapping entries. If you do not specify this keyword, the command displays brief information about NHRP mapping entries.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all NHRP mapping entries.

Examples

Display brief information about all NHRP mapping entries.

```
<Sysname> display nhrp map
Destination/mask  Next hop      NBMA address  Type    Interface
172.16.1.1/32    172.16.1.1    105.112.100.4  cached  Tunnel0
172.16.1.2/32    172.16.1.2    105.112.100.92 cached  Tunnel0
```

Display detailed information about all NHRP mapping entries.

```
<Sysname> display nhrp map verbose
Interface   : Tunnel0
  Destination/mask : 172.16.1.1/32
  Next hop         : 172.16.1.1
  Creation time    : 00:38:44
  Expiration time  : 01:21:15
  Type            : cached
  Flags           : unique, up, used
  NBMA address     : 105.112.100.4

Interface   : Tunnel0
  Destination/mask : 172.16.1.2/32
  Next hop         : 172.16.1.2
  Creation time    : 00:25:53
  Expiration time  : 01:34:06
  Type            : cached
  Flags           : unique, up, used, ipsec
  NBMA address     : 105.112.100.92
```

Table 3 Command output

Field	Description
Destination/mask	Destination tunnel interface address and mask of the mapping entry.
Nexthop	Next hop address to reach the destination network.
Creation time	Period of time for which the mapping entry has been created.
Expiration time	Period of time in which the mapping entry will expire.
Type	Mapping entry type: • static—The entry is statically configured. • cached—The entry is dynamically obtained. • Incomplete—The entry is dynamic and incomplete.
Flags	Mapping entry flags: • unique—The mapping entry in the registration request cannot be overwritten by a mapping entry that has the same protocol address and different public addresses. A client can register the new entry with the server only after the mapping entry on the server expires. • used—This mapping entry is used for packet forwarding. • up—Packets can be forwarded.

Field	Description
	ipsec—IPsec negotiation succeeded. Packets will be protected by IPsec. init—Initialization state.

New command: display nhrp statistics

Use **display nhrp statistics** to display NHRP packet statistics for a tunnel interface.

Syntax

display nhrp statistics [**interface tunnel** *interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface tunnel *interface-number*: Specifies an mGRE tunnel interface by its number in the range of 0 to 4095. If you do not specify this option, the command displays NHRP packet statistics for all tunnel interfaces.

Examples

Display NHRP packet statistics.

```
<Sysname> display nhrp statistics
```

```
Tunnel0:
```

```

NHRP packets sent      : 815
  Resolution requests   : 15
  Resolution replies    : 1
  Registration requests : 0
  Registration replies  : 797
  Purge requests        : 2
  Purge replies         : 0
  Error indications     : 0
  Traffic indications   : 0
```

```

NHRP packets received  : 1453
  Resolution requests   : 15
  Resolution replies    : 1
  Registration requests : 1435
  Registration replies  : 2
  Purge requests        : 0
  Purge replies         : 0
  Error indications     : 0
  Traffic indications   : 0
```

```
Tunnel1:
```

```

NHRP packets sent      : 3
```

```

Resolution Requests      : 0
Resolution replies       : 0
Registration requests     : 0
Registration replies      : 3
Purge requests           : 0
Purge replies            : 0
Error indications        : 0
Traffic indications      : 0

NHRP packets received    : 3
Resolution requests       : 0
Resolution replies        : 0
Registration requests     : 3
Registration replies      : 0
Purge requests           : 0
Purge replies            : 0
Error indications        : 0
Traffic indications      : 0

# Display NHRP packet statistics for the specified tunnel interface.
<Sysname> display nhrp statistics interface tunnel 0
Tunnel0:
  NHRP packets sent       : 815
  Resolution requests      : 15
  Resolution replies       : 1
  Registration requests    : 0
  Registration replies     : 797
  Purge requests           : 2
  Purge replies            : 0
  Error indications        : 0
  Traffic indications      : 0

  NHRP packets received    : 1453
  Resolution requests       : 15
  Resolution replies        : 1
  Registration requests     : 1435
  Registration replies      : 2
  Purge requests           : 0
  Purge replies            : 0
  Error indications        : 0
  Traffic indications      : 0

```

New command: nhrp authentication

Use **nhrp authentication** to configure an NHRP packet authentication key.

Use **undo nhrp authentication** to restore the default.

Syntax

nhrp authentication { cipher | simple } *string*

undo nhrp authentication

Default

No NHRP packet authentication key is configured. NHRP nodes do not authenticate NHRP packets received from each other.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

cipher: Specifies an authentication key in encrypted form.

simple: Specifies an authentication key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key string. Its plaintext form is a case-sensitive string of 1 to 8 characters. Its encrypted form is a case-sensitive string of 1 to 41 characters.

Usage guidelines

After an NHRP packet authentication key is configured for a tunnel interface, the tunnel interface adds the key in packets sent to the peer. The tunnel interface also uses the key to authenticate NHRP packets it receives. If a packet fails the authentication, the packet will be dropped.

For mGRE tunnels to be established successfully, configure the same NHRP authentication key for all NHCs and servers in the same mGRE network.

Examples

```
# On interface Tunnel1, set the NHRP packet authentication key to 123456.
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp authentication simple 123456
```

New command: nhrp holdtime

Use **nhrp holdtime** to configure the holdtime for NHRP mapping entries.

Use **undo nhrp holdtime** to restore the default.

Syntax

nhrp holdtime *seconds*

undo nhrp holdtime

Default

The holdtime of NHRP mapping entries is 7200 seconds.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

seconds: Specifies the holdtime in the range of 1 to 65535 seconds.

Usage guidelines

After the holdtime is configured, the local NHRP holdtime carried in outgoing packets is updated to the configured holdtime.

Examples

```
# On interface Tunnel1, set the holdtime of NHRP mapping entries to 600 seconds
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp holdtime 600
```

New command: nhrp network-id

Use **nhrp network-id** to configure an NHRP network ID for an mGRE tunnel.

Use **undo nhrp network-id** to delete the NHRP network ID of an mGRE tunnel.

Syntax

nhrp network-id *number*

undo nhrp network-id

Default

An mGRE tunnel does not have an NHRP network ID.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

number: Specifies an NHRP network ID in the range of 1 to 4294967295.

Usage guidelines

A network ID is only locally significant. You can configure different NHRP network IDs for different tunnel interfaces on the device. The NHC and server can have different NHRP network IDs.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Set the NHRP network ID to 10 for mGRE tunnel interface Tunnel1.
<Sysname> system-view
[Sysname] interface tunnel 1 mode mgre
[Sysname-Tunnel1] nhrp network-id 10
```

New command: nhrp nhs

Use **nhrp nhs** to configure an NHS private-to-public address mapping.

Use **undo nhrp nhs** to delete an NHS private-to-public address mapping.

Syntax

nhrp nhs *nhs-address* **nbma** *nbma-address*

undo nhrp nhs *nhs-address* **nbma** *nbma-address*

Default

No NHS private-to-public address mappings are configured.

Views

mGRE tunnel interface view

Predefined user roles

network-admin

Parameters

nhs-address: Specifies the private address of an NHS.

nbma-address: Specifies the public address (NBMA address) of the NHS.

Usage guidelines

You can configure multiple NHSs for redundancy. If multiple NHSs are configured, NHCs register with all the NHSs.

Examples

On interface Tunnel1, configure the NHS private address as 1.1.1.1 and public address as 120.1.1.120.

```
<Sysname> system-view
```

```
[Sysname] interface tunnel 1 mode mgre
```

```
[Sysname-Tunnel1] nhrp nhs 1.1.1.1 nbma 120.1.1.120
```

New command: reset mgre session

Use **reset mgre session** to reset dynamic mGRE sessions.

Syntax

reset mgre session [**interface tunnel** *interface-number* [**peer** *ipv4-address*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface tunnel *interface-number*: Specifies an mGRE tunnel interface by its number in the range of 0 to 4095. If you do not specify this option, the command resets dynamic mGRE sessions for all mGRE tunnel interfaces.

peer *ipv4-address*: Specifies a peer public address. If you do not specify this option, the command resets all dynamic mGRE sessions for the specified mGRE tunnel interface.

Usage guidelines

If you do not specify any parameters, this command resets all dynamic mGRE sessions. When an mGRE session is reset, the NHC reregisters with the NHS.

Examples

Reset the mGRE sessions on interface Tunnel1.

```
<Sysname> reset mgre session interface tunnel 1
```

Reset the mGRE session with peer address 202.12.12.12 on interface Tunnel1.

```
<Sysname> reset mgre session interface tunnel 1 peer 202.12.12.12
```

New command: reset mgre statistics

Use **reset mgre statistics** to clear mGRE session statistics.

Syntax

reset mgre statistics [**interface tunnel** *interface-number* [**peer** *ipv4-address*]]

Views

User view

Predefined user roles

network-admin

Parameters

interface tunnel *interface-number*: Specifies an mGRE tunnel interface by its number in the range of 0 to 4095. If you do not specify this option, the command clears mGRE session statistics for all mGRE tunnel interfaces.

peer *ipv4-address*: Specifies a peer public address. If you do not specify this option, the command clears statistics about all mGRE sessions on the specified mGRE tunnel interface.

Examples

Clear statistics about mGRE sessions on interface Tunnel1.

```
<Sysname> reset mgre statistics interface tunnel 1
```

Clear statistics about the mGRE session with peer public address 192.168.1.200 on interface Tunnel1.

```
<Sysname> reset mgre statistics interface tunnel 1 peer 192.168.1.200
```

New command: reset nhrp statistics

Use **reset nhrp statistics** to clear NHRP packet statistics.

Syntax

reset nhrp statistics [**interface tunnel** *interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface tunnel *interface-number*: Specifies an mGRE tunnel interface by its number in the range of 0 to 4095. If you do not specify this option, the command clears NHRP packet statistics for all mGRE tunnel interfaces.

Examples

Clear NHRP packet statistics for interface Tunnel1.

```
<Sysname> reset nhrp statistics interface tunnel 1
```

New feature: Public key management support for Suite B

Configuring Suite B in public key management

Suite B contains a set of encryption and authentication algorithms that meet high security requirements.

In this software version, Suite B is available in public key management. Support for new elliptic curve algorithms was added for generating ECDSA key pairs.

Modified command: public-key local create

Old syntax

```
public-key local create { dsa | ecdsa | rsa } [ name key-name ]
```

New syntax

```
public-key local create { dsa | ecdsa [ secp192r1 | secp256r1 | secp384r1 ] | rsa } [ name key-name ]
```

Views

System view

Change description

Before modification: The secp192r1 curve is used to generate the ECDSA key pair by default. No other elliptic curve algorithms are available.

After modification: You can specify the elliptic curve used to generate the ECDSA key pair. The following elliptic curve algorithms are available:

- **secp192r1**: Uses the secp192r1 curve to generate a 192-bit ECDSA key pair. The secp192r1 curve is used by default.
- **secp256r1**: Uses the secp256r1 curve to generate a 256-bit ECDSA key pair.
- **secp384r1**: Uses the secp384r1 curve to generate a 384-bit ECDSA key pair.

New feature: PKI support for Suite B

Configuring Suite B in PKI

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. In this software version, PKI commands were modified to support Suite B.

Modified command: public-key ecdsa

Old syntax

```
public-key ecdsa name key-name  
undo public-key
```

New syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1**]

undo public-key

Views

PKI domain view

Change description

Before modification: The secp192r1 curve is used to generate the ECDSA key pair by default. No other elliptic curve algorithms are available.

After modification: You can specify the elliptic curve used to generate the ECDSA key pair. The following elliptic curve algorithms are available:

- **secp192r1**: Uses the secp192r1 curve to generate the key pair. The secp192r1 curve is used by default.
- **secp256r1**: Uses the secp256r1 curve to generate the key pair.
- **secp384r1**: Uses the secp384r1 curve to generate the key pair.

New feature: IPsec support for Suite B

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. IPsec provides stronger protection by supporting Suite B and IKEv2.

Overview

Internet Key Exchange version 2 (IKEv2) is an enhanced version of IKEv1. The same as IKEv1, IKEv2 has a set of self-protection mechanisms and can be used on insecure networks for reliable identity authentication, key distribution, and IPsec SA negotiation. IKEv2 provides stronger protection against attacks and higher key exchange ability and needs less message exchanges than IKEv1.

IKEv2 negotiation process

Compared with IKEv1, IKEv2 simplifies the negotiation process and is much more efficient.

IKEv2 defines three types of exchanges: initial exchanges, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange.

As shown in [Figure 11](#), IKEv2 uses two exchanges during the initial exchange process: IKE_SA_INIT and IKE_AUTH, each with two messages.

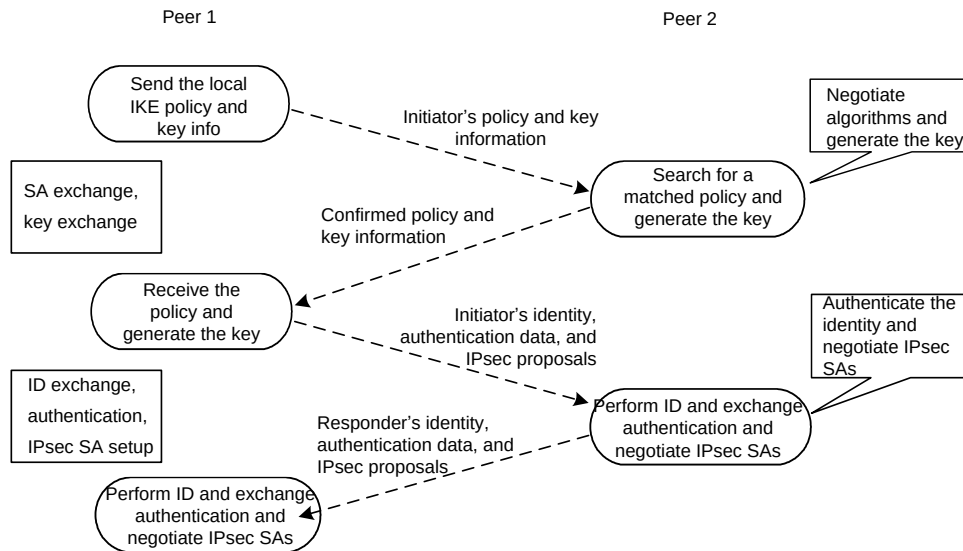
- **IKE_SA_INIT exchange**—Negotiates IKE SA parameters and exchanges keys.
- **IKE_AUTH exchange**—Authenticates the identity of the peer and establishes IPsec SAs.

After the four-message initial exchanges, IKEv2 sets up one IKE SA and one pair of IPsec SAs. For IKEv1 to set up one IKE SA and one pair of IPsec SAs, it must go through two phases that use a minimum of six messages.

To set up one more pair of IPsec SAs within the IKE SA, IKEv2 goes on to perform an additional two-message exchange—the CREATE_CHILD_SA exchange. One CREATE_CHILD_SA exchange creates one pair of IPsec SAs. IKEv2 also uses the CREATE_CHILD_SA exchange to rekey IKE SAs and Child SAs.

IKEv2 uses the INFORMATIONAL exchange to convey control messages about errors and notifications.

Figure 11 IKEv2 Initial exchange process



New features in IKEv2

DH guessing

In the `IKE_SA_INIT` exchange, the initiator guesses the DH group that the responder is most likely to use and sends it in an `IKE_SA_INIT` request message. If the initiator's guess is correct, the responder responds with an `IKE_SA_INIT` response message and the `IKE_SA_INIT` exchange is finished. If the guess is wrong, the responder responds with an `INVALID_KEY_PAYLOAD` message that contains the DH group that it wants to use. The initiator then uses the DH group selected by the responder to reinitiate the `IKE_SA_INIT` exchange. The DH guessing mechanism allows for more flexible DH group configuration and enables the initiator to adapt to different responders.

Cookie challenging

Messages for the `IKE_SA_INIT` exchange are in plain text. An IKEv1 responder cannot confirm the validity of the initiators and must maintain half-open IKE SAs, which makes the responder susceptible to DoS attacks. An attacker can send a large number of `IKE_SA_INIT` requests with forged source IP addresses to the responder, exhausting the responder's system resources.

IKEv2 introduces the cookie challenging mechanism to prevent such DoS attacks. When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new `IKE_SA_INIT` request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

The cookie challenging mechanism automatically stops working when the number of half-open IKE SAs drops below the threshold.

IKEv2 SA rekeying

For security purposes, both IKE SAs and IPsec SAs have a lifetime and must be rekeyed when the lifetime expires. An IKEv1 SA lifetime is negotiated. An IKEv2 SA lifetime, in contrast, is configured. If two peers are configured with different lifetimes, the peer with the shorter lifetime always initiates the SA rekeying. This mechanism reduces the possibility that two peers will simultaneously initiate a rekeying. Simultaneous rekeying results in redundant SAs and SA status inconsistency on the two peers.

IKEv2 message retransmission

Unlike IKEv1 messages, IKEv2 messages appear in request/response pairs. IKEv2 uses the Message ID field in the message header to identify the request/response pair. If an initiator sends a request but receives no response with the same Message ID value within a specific period of time, the initiator retransmits the request.

It is always the IKEv2 initiator that initiates the retransmission, and the retransmitted message must use the same Message ID value.

Protocols and standards

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4718, *IKEv2 Clarifications and Implementation Guidelines*
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*

IKEv2 configuration task list

Determine the following parameters prior to IKEv2 configuration:

- The strength of the algorithms for IKEv2 negotiation, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. Different algorithms provide different levels of protection. A stronger algorithm means better resistance to decryption of protected data but requires more resources. Typically, the longer the key, the stronger the algorithm.
- The local and remote identity authentication methods.
 - To use the pre-shared key authentication method, you must determine the pre-shared key.
 - To use the RSA digital signature authentication method, you must determine the PKI domain for the local end to use. For information about PKI, see PKI configuration in *Security Configuration Guide*.

To configure IKEv2, perform the following tasks:

Tasks at a glance	Remarks
(Required.) Configuring an IKEv2 profile	N/A
(Required.) Configuring an IKEv2 policy	N/A
(Optional.) Configuring an IKEv2 proposal	If you specify an IKEv2 proposal in an IKEv2 policy, you must configure the IKEv2 proposal.
Configuring an IKEv2 keychain	Required when either end or both ends use the pre-shared key authentication method.
Configure global IKEv2 parameters • (Optional.) Enabling the cookie challenging feature • (Optional.) Configuring the IKEv2 DPD feature • (Optional.) Configuring the IKEv2 NAT keepalive feature • (Optional.) Configuring IKEv2 address pools	The cookie challenging feature takes effect only on IKEv2 responders.

Configuring an IKEv2 profile

An IKEv2 profile is intended to provide a set of parameters for IKEv2 negotiation. To configure an IKEv2 profile, perform the following tasks:

1. Specify the local and remote identity authentication methods.

The local and remote identity authentication methods must both be specified and they can be different. You can specify only one local identity authentication method and multiple remote identity authentication methods.
2. Configure the IKEv2 keychain or PKI domain for the IKEv2 profile to use:
 - To use digital signature authentication, configure a PKI domain.
 - To use pre-shared key authentication, configure an IKEv2 keychain.
3. Configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation:
 - For digital signature authentication, the device can use an ID of any type. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses the FQDN as the local ID. The FQDN is the device name configured by using the **sysname** command.
 - For pre-shared key authentication, the device can use an ID of any type other than the DN.
4. Configure peer IDs.

The device compares the received peer ID with the peer IDs of its local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. IKEv2 profiles will be compared in descending order of their priorities.
5. Specify a local interface or IP address for the IKEv2 profile so the profile can be applied only to the specified interface or IP address. For this task, specify the local address configured in IPsec policy or IPsec policy template view (using the **local-address** command). If no local address is configured, specify the IP address of the interface that uses the IPsec policy.
6. Specify a priority number for the IKEv2 profile. To determine the priority of an IKEv2 profile:
 - a. First, the device examines the existence of the **match local** command. An IKEv2 profile with the **match local** command configured has a higher priority.
 - b. If a tie exists, the device compares the priority numbers. An IKEv2 profile with a smaller priority number has a higher priority.
 - c. If a tie still exists, the device prefers an IKEv2 profile configured earlier.
7. Specify a VPN instance for the IKEv2 profile. The IKEv2 profile is used for IKEv2 negotiation only on the interfaces that belong to the VPN instance.
8. Configure the IKEv2 SA lifetime.

The local and remote ends can use different IKEv2 SA lifetimes. They do not negotiate the lifetime. The end with a smaller SA lifetime will initiate an SA negotiation when the lifetime expires.
9. Configure IKEv2 DPD to detect dead IKEv2 peers. You can also configure this feature in system view. If you configure IKEv2 DPD in both views, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.
10. Specify an inside VPN instance. This setting determines where the device should forward received IPsec packets after it de-encapsulates them. If you specify an inside VPN instance, the device looks for a route in the specified VPN instance to forward the packets. If you do not specify an inside VPN instance, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.
11. Configure the NAT keepalive interval.

Configure this task when the device is behind a NAT gateway. The device sends NAT keepalive packets regularly to its peer to prevent the NAT session from being aged because of no matching traffic.

12. Enable the configuration exchange feature.

The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response.

This feature typically applies to scenarios where branches and the headquarters communicate through virtual tunnels.

This feature enables the IPsec gateway at a branch to send IP address requests to the IPsec gateway at the headquarters. When the headquarters receives the request, it sends an IP address to the branch in the response packet. The headquarters can also actively push an IP address to the branch. The branch uses the allocated IP address as the IP address of the virtual tunnel to communicate with the headquarters.

13. Enable AAA authorization.

The AAA authorization feature enables IKEv2 to request authorization attributes, such as the IKEv2 address pool, from AAA. IKEv2 uses the address pool to assign IP addresses to remote users. For more information about AAA authorization, see AAA in *Security Configuration Guide*.

To configure an IKEv2 profile:

Step	Command	Remarks
13. Enter system view.	system-view	N/A
14. Create an IKEv2 profile and enter IKEv2 profile view.	ikev2 profile <i>profile-name</i>	By default, no IKEv2 profiles exist.
15. Configure the local and remote identity authentication methods.	authentication-method { local remote } { dsa-signature ecdsa-signature pre-share rsa-signature }	By default, no local or remote identity authentication method is configured.
16. Specify a keychain.	keychain <i>keychain-name</i>	By default, no keychain is specified for an IKEv2 profile. Perform this task when the pre-shared key authentication method is specified.
17. Specify a PKI domain.	certificate domain <i>domain-name</i> [sign verify]	By default, the device uses PKI domains configured in system view. Perform this task when the digital signature authentication method is specified.
18. Configure the local ID.	identity local { address { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } dn email <i>email-string</i> fqdn <i>fqdn-name</i> key-id <i>key-id-string</i> }	By default, no local ID is configured, and the device uses the IP address of the interface where the IPsec policy applies as the local ID.
19. Configure peer IDs.	match remote { certificate <i>policy-name</i> identity { address { { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] range <i>low-ipv4-address high-ipv4-address</i> } ipv6 { <i>ipv6-address</i> [<i>prefix-length</i>] range <i>low-ipv6-address high-ipv6-address</i> } } fqdn <i>fqdn-name</i> email <i>email-string</i> key-id <i>key-id-string</i> } }	By default, no peer ID is configured. You must configure a minimum of one peer ID on each of the two peers.

Step	Command	Remarks
20. (Optional.) Specify the local interface or IP address to which the IKEv2 profile can be applied.	match local address { <i>interface-type interface-number</i> { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } }	By default, an IKEv2 profile can be applied to any local interface or IP address.
21. (Optional.) Specify a priority for the IKEv2 profile.	priority <i>priority</i>	By default, the priority of an IKEv2 profile is 100.
22. (Optional.) Specify a VPN instance for the IKEv2 profile.	match vrf { name <i>vrf-name</i> any }	By default, an IKEv2 profile belongs to the public network.
23. (Optional.) Set the IKEv2 SA lifetime for the IKEv2 profile.	sa duration <i>seconds</i>	By default, the IKEv2 SA lifetime is 86400 seconds.
24. (Optional.) Configure the DPD feature for the IKEv2 profile.	dpd interval <i>interval</i> [retry <i>seconds</i>] { on-demand periodic }	By default, DPD is disabled for an IKEv2 profile. The global DPD settings in system view are used. If DPD is also disabled in system view, the device does not perform DPD.
25. (Optional.) Specify an inside VPN instance for the IKEv2 profile.	inside-vrf <i>vrf-name</i>	By default, no inside VPN instance is specified for an IKEv2 profile. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.
26. (Optional.) Set the IKEv2 NAT keepalive interval.	nat-keepalive <i>seconds</i>	By default, the global IKEv2 NAT keepalive setting is used.
27. (Optional.) Enable the configuration exchange feature.	config-exchange { request set { accept send } }	By default, all configuration exchange options are disabled.
28. (Optional.) Enable AAA authorization.	aaa authorization domain <i>domain-name</i> username <i>user-name</i>	By default, AAA authorization is disabled for IKEv2.

Configuring an IKEv2 policy

During the IKE_SA_INIT exchange, each end tries to find a matching IKEv2 policy, using the IP address of the local security gateway as the matching criterion.

- If IKEv2 policies are configured, IKEv2 searches for an IKEv2 policy that uses the IP address of the local security gateway. If no IKEv2 policy uses the IP address or the policy is using an incomplete proposal, the IKE_SA_INIT exchange fails.
- If no IKEv2 policy is configured, IKEv2 uses the system default IKEv2 policy **default**.

The device matches IKEv2 policies in the descending order of their priorities. To determine the priority of an IKEv2 policy:

1. First, the device examines the existence of the **match local address** command. An IKEv2 policy with the **match local address** command configured has a higher priority.
2. If a tie exists, the device compares the priority numbers. An IKEv2 policy with a smaller priority number has a higher priority.
3. If a tie still exists, the device prefers an IKEv2 policy configured earlier.

To configure an IKEv2 policy:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 policy and enter IKEv2 policy view.	ikev2 policy <i>policy-name</i>	By default, an IKEv2 policy named default exists.
3. Specify the local interface or address used for IKEv2 policy matching.	match local address { <i>interface-type interface-number</i> { { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } } }	By default, no local interface or address is used for IKEv2 policy matching, and the policy matches any local interface or address.
4. Specify a VPN instance for IKEv2 policy matching.	match vrf { name <i>vrf-name</i> any }	By default, no VPN instance is specified for IKEv2 policy matching. The IKEv2 policy matches all local addresses in the public network.
5. Specify an IKEv2 proposal for the IKEv2 policy.	proposal <i>proposal-name</i>	By default, no IKEv2 proposal is specified for an IKEv2 policy.
6. Specify a priority for the IKEv2 policy.	priority <i>priority</i>	By default, the priority of an IKEv2 policy is 100.

Configuring an IKEv2 proposal

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. An algorithm specified earlier has a higher priority.

A complete IKEv2 proposal must have at least one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

To configure an IKEv2 proposal:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 proposal and enter IKEv2 proposal view.	ikev2 proposal <i>proposal-name</i>	By default, an IKEv2 proposal named default exists. In non-FIPS mode, the default proposal uses the following settings: • Encryption algorithms AES-CBC-128 and 3DES. • Integrity protection algorithms HMAC-SHA1 and HMAC-MD5. • PRF algorithms HMAC-SHA1 and HMAC-MD5. • DH groups 2 and 5. In FIPS mode, the default proposal uses the following settings: • Encryption algorithms AES-CBC-128 and AES-CTR-128. • Integrity protection algorithms HMAC-SHA1 and

Step	Command	Remarks
		HMAC-SHA256. - PRF algorithms HMAC-SHA1 and HMAC-SHA256. - DH groups 14 and 19.
3. Specify the encryption algorithms.	In non-FIPS mode: encryption { 3des-cbc aes-cbc-128 aes-cbc-192 aes-cbc-256 aes-ctr-128 aes-ctr-192 aes-ctr-256 camellia-cbc-128 camellia-cbc-192 camellia-cbc-256 des-cbc } * In FIPS mode: encryption { aes-cbc-128 aes-cbc-192 aes-cbc-256 aes-ctr-128 aes-ctr-192 aes-ctr-256 } *	By default, an IKEv2 proposal does not have any encryption algorithms.
4. Specify the integrity protection algorithms.	In non-FIPS mode: integrity { aes-xcbc-mac md5 sha1 sha256 sha384 sha512 } * In FIPS mode: integrity { sha1 sha256 sha384 sha512 } *	By default, an IKEv2 proposal does not have any integrity protection algorithms.
5. Specify the PRF algorithms.	In non-FIPS mode: prf { aes-xcbc-mac md5 sha1 sha256 sha384 sha512 } * In FIPS mode: prf { sha1 sha256 sha384 sha512 } *	By default, an IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.
6. Specify the DH groups.	In non-FIPS mode: dh { group1 group14 group2 group24 group5 group19 group20 } * In FIPS mode: dh { group14 group24 group19 group20 } *	By default, an IKEv2 proposal does not have any DH groups.

Configuring an IKEv2 keychain

An IKEv2 keychain specifies the pre-shared keys used for IKEv2 negotiation.

An IKEv2 keychain can have multiple IKEv2 peers. Each peer has a symmetric pre-shared key or an asymmetric pre-shared key pair, and information for identifying the peer (such as the peer's host name, IP address or address range, or ID).

An IKEv2 negotiation initiator uses the peer host name or IP address/address range as the matching criterion to search for a peer. A responder uses the peer host IP address/address range or ID as the matching criterion to search for a peer.

To configure an IKEv2 keychain:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create an IKEv2 keychain and enter IKEv2 keychain view.	ikev2 keychain <i>keychain-name</i>	By default, no IKEv2 keychains exist.
3. Create an IKEv2 peer and enter IKEv2 peer view.	peer <i>name</i>	By default, no IKEv2 peers exist.
4. Configure the information for identifying the IKEv2 peer.	- To configure a host name for the peer: hostname <i>host-name</i> - To configure a host IP address or address range for the peer: address { <i>ipv4-address</i> [<i>mask</i> <i>mask-length</i>] ipv6 <i>ipv6-address</i> [<i>prefix-length</i>] } - To configure an ID for the peer: identity { address { <i>ipv4-address</i> ipv6 { <i>ipv6-address</i> } } fqdn <i>fqdn-name</i> email <i>email-string</i> key-id <i>key-id-string</i> }	By default, no hostname, host IP address, address range, or identity information is configured for an IKEv2 peer. You must configure different IP addresses/address ranges for different peers.
5. Configure a pre-shared key for the peer.	pre-shared-key [local remote] { ciphertext plaintext } <i>string</i>	By default, an IKEv2 peer does not have a pre-shared key.

Configure global IKEv2 parameters

Enabling the cookie challenging feature

Enable cookie challenging on responders to protect them against DoS attacks that use a large number of source IP addresses to forge IKE_SA_INIT requests.

To enable cookie challenging:

Step	Command	Remarks
6. Enter system view.	system-view	N/A
7. Enable cookie challenging.	ikev2 cookie-challenge <i>number</i>	By default, IKEv2 cookie challenging is disabled.

Configuring the IKEv2 DPD feature

IKEv2 DPD detects dead IKEv2 peers in periodic or on-demand mode.

- **Periodic DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages at regular intervals.
- **On-demand DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages before sending data.

- Before the device sends data, it identifies the time interval for which the last IPsec packet has been received from the peer. If the time interval exceeds the DPD interval, it sends a DPD message to the peer to detect its liveness.
- If the device has no data to send, it never sends DPD messages.

If you configure IKEv2 DPD in both IKEv2 profile view and system view, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

To configure global IKEv2 DPD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure global IKEv2 DPD.	ikev2 dpd interval <i>interval</i> [retry <i>seconds</i>] { on-demand periodic }	By default, global DPD is disabled.

Configuring the IKEv2 NAT keepalive feature

Configure this feature on the IKEv2 gateway behind the NAT device. The gateway then sends NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

This feature takes effect after the device detects the NAT device.

To configure the IKEv2 NAT keepalive feature:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the IKEv2 NAT keepalive interval.	ikev2 nat-keepalive <i>seconds</i>	By default, the IKEv2 NAT keepalive interval is 10 seconds.

Configuring IKEv2 address pools

To perform centralized management on remote users, an IPsec gateway can use an address pool to assign private IP addresses to remote users.

You must use an IKEv2 address pool together with AAA authorization by specifying the IKEv2 address pool as an AAA authorization attribute. For more information about AAA authorization, see AAA in *Security Configuration Guide*.

To configure IKE address pools:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure an IKEv2 IPv4 address pool.	ikev2 address-group <i>group-name start-ipv4-address end-ipv4-address [mask mask-length]</i>	By default, no IKEv2 IPv4 address pool exists.
3. Configure an IKEv2 IPv6 address pool.	ikev2 ipv6-address-group <i>group-name prefix prefix/prefix-len assign-len assign-len</i>	By default, no IKEv2 IPv6 address pool exists.

Displaying and maintaining IKEv2

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display the IKEv2 proposal configuration.	display ikev2 proposal [<i>name</i> default]
Display the IKEv2 policy configuration.	display ikev2 policy [<i>policy-name</i> default]
Display the IKEv2 profile configuration.	display ikev2 profile [<i>profile-name</i>]
Display the IKEv2 SA information.	display ikev2 sa [[{ local remote } { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-instance-name</i>]] [verbose [tunnel <i>tunnel-id</i>]]
Display IKEv2 statistics.	display ikev2 statistics
Delete IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.	reset ikev2 sa [[{ local remote } { <i>ipv4-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>vpn-instance-name</i>]] tunnel <i>tunnel-id</i>] [fast]
Clear IKEv2 statistics.	reset ikev2 statistics

Command reference

New command: aaa authorization

Use **aaa authorization** to enable IKEv2 AAA authorization.

Use **undo aaa authorization** to disable IKEv2 AAA authorization.

Syntax

aaa authorization domain *domain-name* **username** *user-name*

undo aaa authorization

Default

IKEv2 AAA authorization is disabled.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

domain *domain-name*: Specifies the ISP domain used for requesting authorization attributes. The ISP domain name is a case-insensitive string of 1 to 255 characters and must meet the following requirements:

- The name cannot contain a forward slash (/), backslash (\), vertical bar (|), quotation mark ("), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The name cannot be **d**, **de**, **def**, **defa**, **defau**, **defaul**, **default**, **i**, **if**, **if-**, **if-u**, **if-un**, **if-unk**, **if-unkn**, **if-unkno**, **if-unknow**, or **if-unknown**.

username *user-name*: Specifies the username used for requesting authorization attributes. The username is a case-sensitive string of 1 to 55 characters and must meet the following requirements:

- The username cannot contain the domain name.
- The username cannot contain a forward slash (/), backslash (\), vertical bar (|), colon (:), asterisk (*), question mark (?), left angle bracket (<), right angle bracket (>), or an at sign (@).
- The username cannot be **a**, **al**, or **all**.

Usage guidelines

The AAA authorization feature enables IKEv2 to request authorization attributes, such as the IKEv2 IPv4 address pool, from AAA.

IKEv2 uses the ISP domain and username to request authorization attributes. AAA uses the authorization settings in the ISP domain to request the user's authorization attributes from the remote AAA server or the local user database. After IKEv2 passes the username authentication, it obtains the authorization attributes.

This feature is applicable when AAA is used to centrally manage and deploy authorization attributes.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Enable AAA authorization. Specify the ISP domain name **abc** and the username **test**.

```
[Sysname-ikev2-profile-profile1] aaa authorization domain abc username test
```

Related commands

display ikev2 profile

New command: address

Use **address** to specify the IP address or IP address range of an IKEv2 peer.

Use **undo address** to restore the default.

Syntax

address { *ipv4-address* [*mask* | *mask-length*] | **ipv6** *ipv6-address* [*prefix-length*] }

undo address

Default

An IKEv2 peer's IP address or IP address range is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the IKEv2 peer.

mask: Specifies the subnet mask of the IPv4 address.

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

ipv6 *ipv6-address*: Specifies the IPv6 address of the IKEv2 peer.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

Usage guidelines

Both the initiator and the responder can look up an IKEv2 peer by IP address in IKEv2 negotiation.
The IP addresses of different IKEv2 peers in the same IKEv2 keychain cannot be the same.

Examples

```
# Create an IKEv2 keychain named key1.
<Sysname> system-view
[Sysname] ikev2 keychain key1

# Create an IKEv2 peer named peer1.
[Sysname-ikev2-keychain-key1] peer peer1

# Specify the IKEv2 peer's IP address 3.3.3.3 with the subnet mask 255.255.255.0.
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```

Related commands

- **ikev2 keychain**
- **peer**

New command: authentication-method

Use **authentication-method** to specify the local or remote identity authentication method.

Use **undo authentication-method** to remove the local or remote identity authentication method.

Syntax

```
authentication-method { local | remote } { dsa-signature | ecdsa-signature | pre-share | rsa-signature }
undo authentication-method local
undo authentication-method remote { dsa-signature | ecdsa-signature | pre-share | rsa-signature }
```

Default

No local or remote identity authentication method is specified.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

local: Specifies the local identity authentication method.

remote: Specifies the remote identity authentication method.

dsa-signature: Specifies the DSA signatures as the identity authentication method.

ecdsa-signature: Specifies the ECDSA signatures as the identity authentication method.

pre-share: Specifies the pre-shared key as the identity authentication method.

rsa-signature: Specifies the RSA signatures as the identity authentication method.

Usage guidelines

The local and remote identity authentication methods must both be specified and they can be different.

You can specify only one local identity authentication method. You can specify multiple remote identity authentication methods by executing this command multiple times when there are multiple remote ends whose authentication methods are unknown.

If you use RSA, DSA, or ECDSA signature authentication, you must specify PKI domains for obtaining certificates. You can specify PKI domains by using the **certificate domain** command in IKEv2 profile view. If you do not specify PKI domains in IKEv2 profile view, the PKI domains configured by the **pki domain** command in system view will be used.

If you specify the pre-shared key method, you must specify a pre-shared key for the IKEv2 peer in the keychain used by the IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Specify the pre-shared key and RSA signatures as the local and remote authentication methods, respectively.

```
[Sysname-ikev2-profile-profile1] authentication local pre-share
```

```
[Sysname-ikev2-profile-profile1] authentication remote rsa-signature
```

Specify the PKI domain **gen1** as the PKI domain for obtaining certificates.

```
[Sysname-ikev2-profile-profile1] certificate domain gen1
```

Specify the keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

- **display ikev2 profile**
- **certificate domain** (IKEv2 profile view)
- **keychain** (IKEv2 profile view)

New command: certificate domain

Use **certificate domain** to specify a PKI domain for signature authentication in IKEv2 negotiation.

Use **undo certificate domain** to remove a PKI domain for signature authentication in IKEv2 negotiation.

Syntax

certificate domain *domain-name* [**sign** | **verify**]

undo certificate domain *domain-name*

Default

PKI domains configured in system view are used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters.

sign: Uses the local certificate in the PKI domain to generate a signature.

verify: Uses the CA certificate in the PKI domain to verify the remote end's certificate.

Usage guidelines

If you do not specify the **sign** or **verify** keyword, the PKI domain is used for both **sign** and **verify** purposes. You can specify a PKI domain for each purpose by executing this command multiple times. If you specify the same PKI domain for both purposes, the later configuration takes effect. For example, if you execute **certificate domain abc sign** and **certificate domain abc verify** successively, the PKI domain **abc** will be used only for verification.

If the local end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for signature generation. If the remote end uses RSA, DSA, or ECDSA signature authentication, you must specify a PKI domain for verifying the remote end's certificate. If you do not specify PKI domains, the PKI domains configured in system view will be used.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Specify the PKI domain **abc** for signature. Specify the PKI domain **def** for verification.

```
[Sysname-ikev2-profile-profile1] certificate domain abc sign
```

```
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

Related commands

- **authentication-method**
- **pki domain**

New command: config-exchange

Use **config-exchange** to enable the configuration exchange feature.

Use **undo config-exchange** to disable the configuration exchange feature.

Syntax

```
config-exchange { request | set { accept | send } }
```

```
undo config-exchange { request | set { accept | send } }
```

Default

Configuration exchange is disabled.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

request: Enables the device to send request messages carrying the configuration request payload during the IKE_AUTH exchange.

set: Specifies the configuration set payload exchange.

accept: Enables the device to accept the configuration set payload carried in Info messages.

send: Enables the device to send Info messages carrying the configuration set payload.

Usage guidelines

The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request

and response, and data push and response. The enterprise center can push IP addresses to branches. The branches can request IP addresses, but the requested IP addresses cannot be used.

You can specify both **request** and **set** for the device.

If you specify **request** for the local end, the remote end will respond if it can obtain the requested data through AAA authorization.

If you specify **set send** for the local end, you must specify **set accept** for the remote end.

The device with **set send** specified pushes an IP address after the IKEv2 SA is set up if it does not receive any configuration request from the peer.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Enable the local end to add the configuration request payload to the request message of IKE_AUTH exchange.

```
[Sysname-ikev2-profile-profile1] config-exchange request
```

Related commands

- **aaa authorization**
- **configuration policy**
- **display ikev2 profile**

New command: description

Use **description** to configure a description for an IKE proposal.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

An IKE proposal does not have a description.

Views

IKE proposal view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 80 characters.

Usage guidelines

If multiple IKE proposals exist, you can use this command to configure different descriptions for them to distinguish them.

Examples

Configure the description **test** for the IKE proposal 1.

```
<Sysname> system-view
```

```
[Sysname] ike proposal 1
```

New command: display ike statistics

Use **display ike statistics** to display IKE statistics.

Syntax

display ike statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display IKE statistics.

```
<Sysname> display ike statistics
```

IKE statistics:

```
No matching proposal: 0
Invalid ID information: 0
Unavailable certificate: 0
Unsupported DOI: 0
Unsupported situation: 0
Invalid proposal syntax: 0
Invalid SPI: 0
Invalid protocol ID: 0
Invalid certificate: 0
Authentication failure: 0
Invalid flags: 0
Invalid message id: 0
Invalid cookie: 0
Invalid transform ID: 0
Malformed payload: 0
Invalid key information: 0
Invalid hash information: 0
Unsupported attribute: 0
Unsupported certificate type: 0
Invalid certificate authority: 0
Invalid signature: 0
Unsupported exchange type: 0
No available SA: 0
Retransmit timeout: 0
Not enough memory: 0
Enqueue fails: 0
```

New command: display ikev2 policy

Use **display ikev2 policy** to display the IKEv2 policy configuration.

Syntax

display ikev2 policy [*policy-name* | **default**]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

policy-name: Specifies an IKEv2 policy by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 policy.

Usage guidelines

If you do not specify any parameters, this command displays the configuration of all IKEv2 policies.

Examples

Display the configuration of all IKEv2 policies.

```
<Sysname> display ikev2 policy
IKEv2 policy: 1
  Priority: 100
  Match local address: 1.1.1.1
  Match local address ipv6: 1:1::1:1
  Match VRF: vpn1
  Proposal: 1
  Proposal: 2
IKEv2 policy: default
  Match local address: Any
  Match VRF: Any
  Proposal: default
```

Table 1 Command output

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Priority	Priority of the IKEv2 policy.
Match local address	IPv4 address to which the IKEv2 policy can be applied.
Match local address ipv6	IPv6 address to which the IKEv2 policy can be applied.
Match VRF	VPN instance to which the IKEv2 policy can be applied.
Proposal	IKEv2 proposal that the IKEv2 policy uses.

Related commands

ikev2 policy

New command: display ikev2 profile

Use **display ikev2 profile** to display the IKEv2 profile configuration.

Syntax

display ikev2 profile [*profile-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters. If you do not specify an IKEv2 profile, this command displays the configuration of all IKEv2 profiles.

Examples

Display the configuration of all IKEv2 profiles.

```
<Sysname> display ikev2 profile
IKEv2 profile: 1
  Priority: 100
  Match criteria:
    Local address 1.1.1.1
    Local address GigabitEthernet1/0/1
    Local address 1::1:1:1
    Remote identity address 3.3.3.3/32
    VRF vrf1
  Inside VRF: vrf1
  Local identity: address 1.1.1.1
  Local authentication method: pre-share
  Remote authentication methods: pre-share
  Keychain: Keychain1
  Sign certificate domain:
    Domain1
    abc
  Verify certificate domain:
    Domain2
    YY
  SA duration: 500 seconds
  DPD: Interval 32 secs, retry-interval 23 secs, periodic
  Config exchange: request, set accept, set send
  NAT keepalive: 10 seconds
  AAA authorization: Domain domain1, username ikev2
```

Table 2 Command output

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Priority	Priority of the IKEv2 profile.
Match criteria	Criteria for looking up the IKEv2 profile.
Inside vrf	Inside VPN instance.

Field	Description
Local identity	ID of the local end.
Local authentication method	Method that the local end uses for authentication.
Remote authentication methods	Methods that the remote end uses for authentication.
Keychain	IKEv2 keychain that the IKEv2 profile uses.
Sign certificate domain	PKI domain used for signature generation.
Verify certificate domain	PKI domain used for verifying the remote end's certificate.
SA duration	Lifetime of the IKEv2 SA.
DPD	DPD settings: - Detection interval in seconds. - Retry interval in seconds. - Detection mode, on demand or periodically. If DPD is disabled, this field displays Disabled .
Config exchange	Configuration exchange settings: request—The local end sends request messages carrying the configuration request payload during the IKE_AUTH exchange. set accept—The local end accepts the configuration set payload carried in Info messages. set send—The local end sends Info messages carrying the configuration set payload.
NAT keepalive	NAT keepalive interval in seconds.
AAA authorization	AAA authorization settings: - ISP domain name. - Username.

Related commands

ikev2 profile

New command: display ikev2 proposal

Use **display ikev2 proposal** to display the IKEv2 proposal configuration.

Syntax

display ikev2 proposal [*name* | **default**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

default: Specifies the default IKEv2 proposal.

Usage guidelines

This command displays IKEv2 proposals in descending order of priorities. If you do not specify any parameters, this command displays the configuration of all IKEv2 proposals.

Examples

Display the configuration of all IKEv2 proposals.

```
<Sysname> display ikev2 proposal
```

```
IKEv2 proposal: 1
```

```
Encryption: 3DES-CBC, AES-CBC-128, AES-CTR-192, CAMELLIA-CBC-128
```

```
Integrity: MD5, SHA256, AES-XCBC
```

```
PRF: MD5, SHA256, AES-XCBC
```

```
DH group: MODP1024/Group 2, MODP1536/Group 5
```

```
IKEv2 proposal: default
```

```
Encryption: AES-CBC-128, 3DES-CBC
```

```
Integrity: SHA1, MD5
```

```
PRF: SHA1, MD5
```

```
DH group: MODP1536/Group 5, MODP1024/Group 2
```

Table 3 Command output

Field	Description
IKEv2 proposal	Name of the IKEv2 proposal.
Encryption	Encryption algorithms that the IKEv2 proposal uses.
Integrity	Integrity protection algorithms that the IKEv2 proposal uses.
PRF	PRF algorithms that the IKEv2 proposal uses.
DH group	DH groups that the IKEv2 proposal uses.

Related commands

ikev2 proposal

New command: display ikev2 sa

Use **display ikev2 sa** to display the IKEv2 SA information.

Syntax

```
display ikev2 sa [ { count | local | remote } { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] ] [ verbose [ tunnel tunnel-id ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

count: Displays the number of IKEv2 SAs.

local: Displays IKEv2 SA information for a local IP address.

remote: Displays IKEv2 SA information for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 ipv6-address: Specifies a local or remote IPv6 address.

vpn-instance vpn-instance-name: Displays information about the IKEv2 SAs in an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays information about IKEv2 SAs for the public network.

verbose: Displays detailed information. If you do not specify this keyword, the command displays the summary information.

tunnel tunnel-id: Displays detailed IKEv2 SA information for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

Usage guidelines

If you do not specify any parameters, this command displays summary information about all IKEv2 SAs.

Examples

Display summary information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	1.1.1.2/500	EST
2	2.2.2.1/500	2.2.2.2/500	EST

Status:
IN-NEGO: Negotiating, EST: Established, DEL: Deleting

Display summary IKEv2 SA information for the remote IP address 1.1.1.2.

```
<Sysname> display ikev2 sa remote 1.1.1.2
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	1.1.1.2/500	EST

Status:
IN-NEGO: Negotiating, EST: Established, DEL: Deleting

Table 4 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local	Local IP address of the IKEv2 SA.
Remote	Remote IP address of the IKEv2 SA.
Status	Status of the IKEv2 SA: • IN-NEGO (Negotiating)—The IKEv2 SA is under negotiation. • EST (Established)—The IKEv2 SA has been set up. • DEL (Deleting)—The IKEv2 SA is about to be deleted.

Display detailed information about all IKEv2 SAs.

```
<Sysname> display ikev2 sa verbose
```

Tunnel ID: 1
Local IP/Port: 1.1.1.1/500
Remote IP/Port: 1.1.1.2/500
Outside VRF: -

Inside VRF: -
Local SPI: 8f8af3dbf5023a00
Remote SPI: 0131565b9b3155fa

Local ID type: FQDN
Local ID: router_a
Remote ID type: FQDN
Remote ID: router_b

Auth sign method: Pre-shared key
Auth verify method: Pre-shared key
Integrity algorithm: HMAC_MD5
PRF algorithm: HMAC_MD5
Encryption algorithm: AES-CBC-192

Life duration: 86400 secs
Remaining key duration: 85604 secs
Diffie-Hellman group: MODP1024/Group2
NAT traversal: Not detected
DPD: Interval 20 secs, retry interval 2 secs
Transmitting entity: Initiator

Local window: 1
Remote window: 1
Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24

Display detailed IKEv2 SA information for the remote IP address 1.1.1.2.

<Sysname> display ikev2 sa remote 1.1.1.2 verbose

Tunnel ID: 1
Local IP/Port: 1.1.1.1/500
Remote IP/Port: 1.1.1.2/500
Outside VRF: -
Inside VRF: -
Local SPI: 8f8af3dbf5023a00
Remote SPI: 0131565b9b3155fa

Local ID type: FQDN
Local ID: router_a
Remote ID type: FQDN
Remote ID: router_b

Auth sign method: Pre-shared key

Auth verify method: Pre-shared key
Integrity algorithm: HMAC_MD5
PRF algorithm: HMAC_MD5
Encryption algorithm: AES-CBC-192

Life duration: 86400 secs
Remaining key duration: 85604 secs
Diffie-Hellman group: MODP1024/Group2
NAT traversal: Not detected
DPD: Interval 30 secs, retry 10 secs
Transmitting entity: Initiator

Local window: 1
Remote window: 1
Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24

Table 5 Command output

Field	Description
Tunnel ID	ID of the IPsec tunnel to which the IKEv2 SA belongs.
Local IP/Port	IP address and port number of the local security gateway.
Remote IP/Port	IP address and port number of the remote security gateway.
Outside VRF	Name of the VPN instance to which the protected outbound data flow belongs. If the protected outbound data flow belongs to the public network, this field displays a hyphen (-).
Inside VRF	Name of the VPN instance to which the protected inbound data flow belongs. If the protected inbound data flow belongs to the public network, this field displays a hyphen (-).
Local SPI	SPI that the local end uses.
Remote SPI	SPI that the remote end uses.
Local ID type	ID type of the local security gateway.
Local ID	ID of the local security gateway.
Remote ID type	ID type of the remote security gateway.
Remote ID	ID of the remote security gateway.
Auth sign method	Signature method that the IKEv2 proposal uses in authentication.
Auth verify method	Verification method that the IKEv2 proposal uses in authentication.
Integrity algorithm	Integrity protection algorithms that the IKEv2 proposal uses.

Field	Description
PRF algorithm	PRF algorithms that the IKEv2 proposal uses.
Encryption algorithm	Encryption algorithms that the IKEv2 proposal uses.
Life duration	Lifetime of the IKEv2 SA, in seconds.
Remaining key duration	Remaining lifetime of the IKEv2 SA, in seconds.
Diffie-Hellman group	DH groups used in IKEv2 key negotiation.
NAT traversal	Whether a NAT gateway is detected between the local and remote ends.
DPD	DPD settings: - Detection interval in seconds. - Retry interval in seconds. If DPD is disabled, this field displays Disabled .
Transmitting entity	Role of the local end in IKEv2 negotiation, initiator or responder.
Local window	Window size that the local end uses.
Remote window	Window size that the remote end uses.
Local request message ID	ID of the request message that the local end is about to send.
Remote request message ID	ID of the request message that the remote end is about to send.
Local next message ID	ID of the message that the local end expects to receive.
Remote next message ID	ID of the message that the remote end expects to receive.
Pushed IP address	IP address pushed to the local end by the remote end.
Assigned IP address	IP address assigned to the remote end by the local end .

New command: display ikev2 statistics

Use **display ikev2 statistics** to display IKEv2 statistics.

Syntax

display ikev2 statistics

Views

Any view

Predefined user roles

network-admin
network-operator

Examples

```
# Display IKEv2 statistics.
<Sysname> display ikev2 statistics
IKEv2 statistics:
  Unsupported critical payload: 0
  Invalid IKE SPI: 0
  Invalid major version: 0
```

```

Invalid syntax: 0
Invalid message ID: 0
Invalid SPI: 0
No proposal chosen: 0
Invalid KE payload: 0
Authentication failed: 0
Single pair required: 0
TS unacceptable: 0
Invalid selectors: 0
Temporary failure: 0
No child SA: 0
Unknown other notify: 0
No enough resource: 0
Enqueue error: 0
No IKEv2 SA: 0
Packet error: 0
Other error: 0
Retransmit timeout: 0
DPD detect error: 0
Del child for IPsec message: 0
Del child for deleting IKEv2 SA: 0
Del child for receiving delete message: 0

```

New command: dh

Use **dh** to specify DH groups to be used in IKEv2 key negotiation.

Use **undo group** to restore the default.

Syntax

In non-FIPS mode:

```
dh { group1 | group14 | group2 | group24 | group5 | group19 | group20 } *
```

```
undo dh
```

In FIPS mode:

```
dh { group14 | group24 | group19 | group20 } *
```

```
undo dh
```

Default

No DH group is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

group1: Uses the 768-bit Diffie-Hellman group.

group2: Uses the 1024-bit Diffie-Hellman group.

group5: Uses the 1536-bit Diffie-Hellman group.

group14: Uses the 2048-bit Diffie-Hellman group.

group24: Uses the 2048-bit Diffie-Hellman group with the 256-bit prime order subgroup.

group19: Uses the 256-bit ECP Diffie-Hellman group.

group20: Uses the 384-bit ECP Diffie-Hellman group.

Usage guidelines

A DH group with a higher group number provides higher security but needs more time for processing. To achieve the best trade-off between processing performance and security, choose proper DH groups for your network.

You must specify a minimum of one DH group for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless.

You can specify multiple DH groups for an IKEv2 proposal. A group specified earlier has a higher priority.

Examples

```
# Specify DH groups 1 for the IKEv2 proposal 1.
```

```
<Sysname> system-view
```

```
[Sysname] ikev2 proposal 1
```

```
[Sysname-ikev2-proposal-1] dh group1
```

Related commands

ikev2 proposal

New command: dpd

Use **dpd** to configure the IKEv2 DPD feature.

Use **undo dpd** to disable the IKEv2 DPD feature.

Syntax

dpd interval *interval* [**retry seconds**] { **on-demand** | **periodic** }

undo dpd interval

Default

IKEv2 DPD is disabled. The global IKEv2 DPD settings are used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry seconds: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

Examples

```
# Configure on-demand IKEv2 DPD. Set the DPD triggering interval to 10 seconds and the retry interval to 5 seconds.
```

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

Related commands

ikev2 dpd

New command: encryption

Use **encryption** to specify encryption algorithms for an IKEv2 proposal.

Use **undo encryption** to restore the default.

Syntax

In non-FIPS mode:

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-ctr-128 | aes-ctr-192 | aes-ctr-256 | camellia-cbc-128 | camellia-cbc-192 | camellia-cbc-256 | des-cbc } *
```

undo encryption

In FIPS mode:

```
encryption { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-ctr-128 | aes-ctr-192 | aes-ctr-256 } *
```

undo encryption

Default

No encryption algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the 3DES algorithm in CBC mode, which uses a 168-bit key.

aes-cbc-128: Specifies the AES algorithm in CBC mode, which uses a 128-bit key.

aes-cbc-192: Specifies the AES algorithm in CBC mode, which uses a 192-bit key.

aes-cbc-256: Specifies the AES algorithm in CBC mode, which uses a 256-bit key.

aes-ctr-128: Specifies the AES algorithm in CTR mode, which uses a 128-bit key.

aes-ctr-192: Specifies the AES algorithm in CTR mode, which uses a 192-bit key.

aes-ctr-256: Specifies the AES algorithm in CTR mode, which uses a 256-bit key.

camellia-cbc-128: Specifies the Camellia algorithm in CBC mode, which uses a 128-bit key.

camellia-cbc-192: Specifies the Camellia algorithm in CBC mode, which uses a 192-bit key.

camellia-cbc-256: Specifies the Camellia algorithm in CBC mode, which uses a 256-bit key.

des-cbc: Specifies the DES algorithm in CBC mode, which uses a 56-bit key.

Usage guidelines

You must specify a minimum of one encryption algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple encryption algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Specify the 168-bit 3DES algorithm in CBC mode as the encryption algorithm for the IKE proposal **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption-algorithm 3des-cbc
```

Related commands

ikev2 proposal

New command: hostname

Use **hostname** to specify the host name of an IKEv2 peer.

Use **undo hostname** to restore the default.

Syntax

hostname *name*

undo hostname

Default

An IKEv2 peer's host name is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

name: Specifies the host name of the IKEv2 peer, a case-insensitive string of 1 to 253 characters.

Usage guidelines

Only the initiator can look up an IKEv2 peer by host name in IKEv2 negotiation, and the initiator must use an IPsec policy rather than an IPsec profile.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the host name **test** of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

Related commands

- **ikev2 keychain**
- **peer**

New command: identity

Use **identity** to specify the ID of an IKEv2 peer.

Use **undo identity** to restore the default.

Syntax

identity { **address** { *ipv4-address* | **ipv6** { *ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* }

undo identity

Default

An IKEv2 peer's ID is not specified.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the peer.

ipv6 *ipv6-address*: Specifies the IPv6 address of the peer.

fqdn *fqdn-name*: Specifies the FQDN of the peer. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as *www.test.com*.

email *email-string*: Specifies the email address of the peer. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as *esec@test.com*.

key-id *key-id-string*: Specifies the remote gateway's key ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Only the responder can look up an IKEv2 peer by ID in IKEv2 negotiation. The initiator does not know the peer ID when initiating the IKEv2 negotiation, so it cannot use an ID for IKEv2 peer lookup.

Examples

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Specify the peer IPv4 address 1.1.1.2 as the ID of the IKEv2 peer.

```
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

Related commands

- **ikev2 keychain**
- **peer**

New command: identity local

Use **identity local** to configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation.

Use **undo identity local** to restore the default.

Syntax

identity local { **address** { *ipv4-address* | **ipv6** *ipv6-address* } | **dn** | **email** *email-string* | **fqdn** *fqdn-name* | **key-id** *key-id-string* }

undo identity local

Default

No local ID is specified. The IP address of the interface to which the IPsec policy is applied is used as the local ID.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

address { *ipv4-address* | **ipv6** *ipv6-address* }: Uses an IPv4 or IPv6 address as the local ID.

dn: Uses the DN in the local certificate as the local ID.

email *email-string*: Uses an email address as the local ID. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as sec@abc.com.

fqdn *fqdn-name*: Uses an FQDN as the local ID. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as www.test.com.

key-id *key-id-string*: Uses the device's key ID as the local ID. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

Peers exchange local IDs for identifying each other in negotiation.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Use the IP address 2.2.2.2 as the local ID.

```
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

Related commands

peer

New command: ikev2 address-group

Use **ikev2 address-group** to configure an IKEv2 IPv4 address pool for assigning IPv4 addresses to remote peers.

Use **undo ikev2 address-group** to delete an IKEv2 IPv4 address pool.

Syntax

ikev2 address-group *group-name start-ipv4-address end-ipv4-address [mask | mask-length]*
undo ikev2 address-group *group-name*

Default

No IKEv2 IPv4 address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies an name for the IKEv2 IPv4 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

start-ipv4-address end-ipv4-address: Specifies an IPv4 address range. The *start-ipv4-address* argument specifies the start IPv4 address. The *end-ipv4-address* argument specifies the end IPv4 address.

mask: Specifies the IPv4 address mask.

mask-length: Specifies the length of the IPv4 address mask.

Usage guidelines

An IKE IPv4 address pool can contain a maximum of 8192 IPv4 addresses.

Examples

Configure an IKEv2 IPv4 address pool with the name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and the mask 255.255.255.0.

```
<Sysname> system-view
```

```
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 255.255.255.0
```

Configure an IKEv2 IPv4 address pool with the name **ipv4group**, address range 1.1.1.1 to 1.1.1.2, and the mask length 32.

```
<Sysname> system-view
```

```
[Sysname] ikev2 address-group ipv4group 1.1.1.1 1.1.1.2 32
```

Related commands

address-group

New command: ikev2 cookie-challenge

Use **ikev2 cookie-challenge** to enable the cookie challenging feature.

Use **undo ikev2 cookie-challenge** to disable the cookie challenging feature.

Syntax

ikev2 cookie-challenge *number*
undo ikev2 cookie-challenge

Default

The cookie challenging feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the threshold for triggering the cookie challenging feature. The value range for this argument is 0 to 1000 half-open IKE SAs.

Usage guidelines

When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

This feature can protect the responder against DoS attacks which aim to exhaust the responder's system resources by using a large number of IKE_SA_INIT requests with forged source IP addresses.

Examples

```
# Enable the cookie challenging feature and set the threshold to 450.
```

```
<Sysname> system-view
```

```
[Sysname] ikev2 cookie-challenge 450
```

New command: ikev2 dpd

Use **ikev2 dpd** to configure the global IKEv2 DPD feature.

Use **undo ikev2 dpd** to disable the global IKEv2 DPD feature.

Syntax

ikev2 dpd interval *interval* [**retry** *seconds*] { **on-demand** | **periodic** }

undo ikev2 dpd interval

Default

The global IKEv2 DPD feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a DPD triggering interval in the range of 10 to 3600 seconds.

retry *seconds*: Specifies the DPD retry interval in the range of 2 to 60 seconds. The default is 5 seconds.

on-demand: Triggers DPD on demand. The device triggers DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for the specified interval.

periodic: Triggers DPD at regular intervals. The device triggers DPD at the specified interval.

Usage guidelines

DPD is triggered periodically or on-demand. The on-demand mode is recommended when the device communicates with a large number of IKEv2 peers. For an earlier detection of dead peers, use the periodic triggering mode, which consumes more bandwidth and CPU.

The triggering interval must be longer than the retry interval, so that the device will not trigger a new round of DPD during a DPD retry.

You can configure IKEv2 DPD in both IKEv2 profile view and system view. The IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

Examples

Configure the device to trigger IKEv2 DPD if it has IPsec traffic to send and has not received any IPsec packets from the peer for 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 on-demand
```

Configure the device to trigger IKEv2 DPD every 15 seconds.

```
<Sysname> system-view
[Sysname] ikev2 dpd interval 15 periodic
```

Related commands

dpd (IKEv2 profile view)

New command: ikev2 ipv6-address-group

Use **ikev2 ipv6-address-group** to configure an IKEv2 IPv6 address pool for assigning IPv6 addresses to remote peers.

Use **undo ikev2 ipv6-address-group** to delete an IKEv2 IPv6 address pool.

Syntax

ikev2 ipv6-address-group *group-name* **prefix** *prefix/prefix-len* **assign-len** *assign-len*
undo ikev2 ipv6-address-group *group-name*

Default

No IKEv2 IPv6 address pools exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies a name for the IKEv2 IPv6 address pool. The *group-name* argument is a case-insensitive string of 1 to 63 characters.

prefix *prefix/prefix-len*: Specifies an IPv6 prefix in the format of *prefix/prefix length*. The value range for the *prefix-len* argument is 1 to 128.

assign-len *assign-len*: Specifies the assigned prefix length. The value range for the *assign-len* argument is 0 to 128, and the value must be greater than or equal to *prefix-len*. The difference between *assign-len* and *prefix-len* must be no more than 16.

Usage guidelines

Different from the IKEv2 IPv4 address pool, the device assigns an IPv6 subnet to a peer from the IKEv2 IPv6 address pool. The peer can use the assigned IPv6 subnet to assign IPv6 addresses to other devices.

IKEv2 IPv6 address pools cannot overlap with each other.

Examples

Configure an IKEv2 IPv6 address pool with the name **ipv6group**, prefix 1:1::/64, and the assigned prefix length 80.

```
<Sysname> system-view
```

```
[Sysname] ikev2 ipv6-address-group ipv6group prefix :1:1::/64 assign-len 80
```

Related commands

ipv6-address-group

New command: ikev2 keychain

Use **ikev2 keychain** to create an IKEv2 keychain and enter its view, or enter the view of an existing IKEv2 keychain.

Use **undo ikev2 keychain** to delete an IKEv2 keychain.

Syntax

ikev2 keychain *keychain-name*

undo ikev2 keychain *keychain-name*

Default

No IKEv2 keychains exist.

Views

System view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies a name for the IKEv2 keychain. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses pre-shared key authentication. The pre-shared key configured on both ends must be the same.

You can configure multiple IKEv2 peers in an IKEv2 keychain.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain key1
```

```
[Sysname-ikev2-keychain-key1]
```

New command: ikev2 nat-keepalive

Use **ikev2 nat-keepalive** to set the NAT keepalive interval.

Use **undo ikev2 nat-keepalive** to restore the default.

Syntax

ikev2 nat-keepalive *seconds*

undo ikev2 nat-keepalive

Default

The NAT keepalive interval is 10 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
```

```
[Sysname] ikev2 nat-keepalive 5
```

New command: ikev2 policy

Use **ikev2 policy** to create an IKEv2 policy and enter its view, or enter the view of an existing IKEv2 policy.

Use **undo ikev2 policy** to delete an IKEv2 policy.

Syntax

ikev2 policy *policy-name*

undo ikev2 policy *policy-name*

Default

An IKEv2 policy named **default** exists, which uses the default IKEv2 proposal and matches any local addresses.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the IKEv2 policy. The policy name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied and the VPN instance to which the interface belongs. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet and the VPN instance to which the interface belongs. An IKEv2 policy uses IKEv2 proposals to define the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups to be used for negotiation.

You can configure multiple IKEv2 policies. An IKEv2 policy must have a minimum of one IKEv2 proposal. Otherwise, the policy is incomplete.

If the initiator uses an IPsec policy that is bound to a source interface, the initiator looks up an IKEv2 policy by the IP address of the source interface.

You can set priorities to adjust the match order of IKEv2 policies that have the same match criteria.

If no IKEv2 policy is configured, the default IKEv2 policy is used. You cannot enter the view of the default IKEv2 policy, nor modify it.

Examples

Create an IKEv2 policy named **policy1** and enter IKEv2 policy view.

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

Related commands

display ikev2 policy

New command: ikev2 profile

Use **ikev2 profile** to create an IKEv2 profile and enter its view, or enter the view of an existing IKEv2 profile.

Use **undo ikev2 profile** to delete an IKEv2 profile.

Syntax

ikev2 profile *profile-name*

undo ikev2 profile *profile-name*

Default

No IKEv2 profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a name for the IKEv2 profile. The profile name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 profile contains the IKEv2 SA parameters that are not negotiated, such as the identity information and authentication methods of the peers, and the matching criteria for profile lookup.

Examples

Create an IKEv2 profile named **profile1** and enter IKEv2 profile view.

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```

Related commands

display ikev2 profile

New command: ikev2 proposal

Use **ikev2 proposal** to create an IKEv2 proposal and enter its view, or enter the view of an existing IKEv2 proposal.

Use **undo ikev2 proposal** to delete an IKEv2 proposal.

Syntax

ikev2 proposal *proposal-name*

undo ikev2 proposal *proposal-name*

Default

An IKEv2 proposal named **default** exists, which has the lowest priority and uses the following settings:

- In non-FIPS mode:
 - **Encryption algorithm**—AES-CBC-128 and 3DES.
 - **Integrity protection algorithm**—HMAC-SHA1 and HMAC-MD5.
 - **PRF algorithm**—HMAC-SHA1 and HMAC-MD5.
 - **DH group**—Group 5 and group 2.
- In FIPS mode:
 - **Encryption algorithm**—AES-CBC-128 and AES-CTR-128.
 - **Integrity protection algorithm**—HMAC-SHA1 and HMAC-SHA256.
 - **PRF algorithm**—HMAC-SHA1 and HMAC-SHA256.
 - **DH group**—Group 14 and group 19.

Views

System view

Predefined user roles

network-admin

Parameters

proposal-name: Specifies a name for the IKEv2 proposal. The proposal name is a case-insensitive string of 1 to 63 characters and cannot be **default**.

Usage guidelines

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups.

An IKEv2 proposal must have a minimum of one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

In an IKEv2 proposal, you can specify multiple parameters of the same type. The parameters of different types combine and form multiple sets of security parameters. If you want to use only one set of security parameters, configure only one set of security parameters for the IKEv2 proposal.

Examples

Create an IKEv2 proposal named **prop1**. Specify the encryption algorithm AES-CBC-128, integrity protection algorithm SHA1, PRF algorithm SHA1, and DH group 2.

```
<Sysname> system-view
```

```
[Sysname] ikev2 proposal prop1
```

```
[Sysname-ikev2-proposal-prop1] encryption-algorithm aes-cbc-128
```

```
[Sysname-ikev2-proposal-prop1] authentication-algorithm sha1
```

```
[Sysname-ikev2-proposal-prop1] prf sha1
```

```
[Sysname-ikev2-proposal-prop1] dh group2
```

Related commands

- **encryption-algorithm**
- **integrity**
- **prf**
- **dh**

New command: inside-vrf

Use **inside-vrf** to specify an inside VPN instance.

Use **undo inside-vrf** to restore the default.

Syntax

inside-vrf *vrf-name*

undo inside-vrf

Default

No inside VPN instance is specified. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

vrf-name: Specifies the VPN instance to which the protected data belongs. The *vrf-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

This command determines where the device should forward received IPsec packets after it de-encapsulates them. If you configure this command, the device looks for a route in the specified VPN instance to forward the packets. If you do not configure this command, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Specify the inside VPN instance **vpn1**.

```
[Sysname-ikev2-profile-profile1] inside-vrf vpn1
```

New command: integrity

Use **integrity** to specify integrity protection algorithms for an IKEv2 proposal.

Use **undo integrity** to restore the default.

Syntax

In non-FIPS mode:

```
integrity { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 } *
```

```
undo integrity
```

In FIPS mode:

```
integrity { sha1 | sha256 | sha384 | sha512 } *
```

```
undo integrity
```

Default

No integrity protection algorithm is specified for an IKEv2 proposal.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You must specify a minimum of one integrity protection algorithm for an IKEv2 proposal. Otherwise, the proposal is incomplete and useless. You can specify multiple integrity protection algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

```
# Create an IKEv2 proposal named prop1.
```

```
<Sysname> system-view
```

```
[Sysname] ikev2 proposal prop1
```

```
# Specify HMAC-SHA1 and HMAC-MD5 as the integrity protection algorithms, with HMAC-SHA1 preferred.
```

```
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

Related commands

```
ikev2 proposal
```

New command: keychain

Use **keychain** to specify an IKEv2 keychain for pre-shared key authentication.

Use **undo keychain** to restore the default.

Syntax

```
keychain keychain-name
```

```
undo keychain
```

Default

No IKEv2 keychain is specified for an IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

keychain-name: Specifies an IKEv2 keychain by its name. The keychain name is a case-insensitive string of 1 to 63 characters and cannot contain a hyphen (-).

Usage guidelines

An IKEv2 keychain is required on both ends if either end uses pre-shared key authentication. You can specify only one IKEv2 keychain for an IKEv2 profile.

You can specify the same IKEv2 keychain for different IKEv2 profiles.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Specify the IKEv2 keychain **keychain1**.

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

Related commands

- **display ikev2 profile**
- **ikev2 keychain**

New command: match local (IKEv2 profile view)

Use **match local** to specify a local interface or a local IP address to which an IKEv2 profile can be applied.

Use **undo match local** to remove a local interface or a local IP address to which an IKEv2 profile can be applied.

Syntax

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

Default

An IKEv2 profile can be applied to any local interface or IP address.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

address: Specifies a local interface or IP address to which an IKEv2 profile can be applied.

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

Use this command to specify which address or interface can use the IKEv2 profile for IKEv2 negotiation. The interface is the interface that receives IKEv2 packets. The IP address is the IP address of the interface that receives IKEv2 packets.

An IKEv2 profile configured earlier has a higher priority. To give an IKEv2 profile that is configured later a higher priority, you can configure the **priority** command or this command for the profile. For example, suppose you configured IKEv2 profile A before configuring IKEv2 profile B, and you configured the **match remote identity address range 2.2.2.1 2.2.2.100** command for IKEv2 profile A and the **match remote identity address range 2.2.2.1 2.2.2.10** command for IKEv2 profile B. For the local interface with the IP address 3.3.3.3 to negotiate with the peer 2.2.2.6, IKEv2 profile A is preferred because IKEv2 profile A was configured earlier. To use IKEv2 profile B, you can use this command to restrict the application scope of IKEv2 profile B to IPv4 address 3.3.3.3.

You can specify multiple applicable local interfaces or IP addresses for an IKEv2 profile.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Apply the IKEv2 profile **profile1** to the interface whose IP address is 2.2.2.2.

```
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

Related commands

match remote

New command: match local address (IKEv2 policy view)

Use **match local address** to specify a local interface or a local address that an IKEv2 policy matches.

Use **undo match local address** to remove a local interface or a local address that an IKEv2 policy matches.

Syntax

match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

undo match local address { *interface-type interface-number* | { *ipv4-address* | **ipv6** *ipv6-address* } }

Default

No local interface or address is specified, and the IKEv2 policy matches any local interface or address.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a local interface by its type and number. It can be any Layer 3 interface.

ipv4-address: Specifies the IPv4 address of a local interface.

ipv6 *ipv6-address*: Specifies the IPv6 address of a local interface.

Usage guidelines

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Configure the IKEv2 policy **policy1** to match the local address 3.3.3.3.

```
<Sysname> system-view
```

```
[Sysname] ikev2 policy policy1
```

```
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

Related commands

- **display ikev2 policy**
- **match vrf**

New command: match remote

Use **match remote** to configure a peer ID that an IKEv2 profile matches.

Use **undo match remote** to delete a peer ID that an IKEv2 profile matches.

Syntax

match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address* *high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address* *high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }

undo match remote { **certificate** *policy-name* | **identity** { **address** { { *ipv4-address* [*mask* | *mask-length*] | **range** *low-ipv4-address* *high-ipv4-address* } | **ipv6** { *ipv6-address* [*prefix-length*] | **range** *low-ipv6-address* *high-ipv6-address* } } | **fqdn** *fqdn-name* | **email** *email-string* | **key-id** *key-id-string* } }

Default

No matching peer ID is configured for an IKEv2 profile.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

certificate *policy-name*: Uses the information in the peer's digital certificate as the peer ID for IKEv2 profile matching. The *policy-name* argument specifies a certificate-based access control policy by its name, a case-insensitive string of 1 to 31 characters.

identity: Uses the specified information as the peer ID for IKEv2 profile matching. The specified information is configured on the peer by using the **identity local** command.

- **address** *ipv4-address* [*mask* | *mask-length*]: Uses an IPv4 host address or an IPv4 subnet address as the peer ID for IKEv2 profile matching. The value range for the *mask-length* argument is 0 to 32.
- **address range** *low-ipv4-address* *high-ipv4-address*: Uses a range of IPv4 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.
- **address ipv6** *ipv6-address* [*prefix-length*]: Uses an IPv6 host address or an IPv6 subnet address as the peer ID for IKEv2 profile matching. The value range for the *prefix-length* argument is 0 to 128.
- **address ipv6 range** *low-ipv6-address* *high-ipv6-address*: Uses a range of IPv6 addresses as the peer ID for IKEv2 profile matching. The end address must be higher than the start address.

- **fqdn** *fqdn-name*: Uses the peer's FQDN as the peer ID for IKEv2 profile matching. The *fqdn-name* argument is a case-sensitive string of 1 to 255 characters, such as `www.test.com`.
- **email** *email-string*: Uses peer's email address as the peer ID for IKEv2 profile matching. The *email-string* argument is a case-sensitive string of 1 to 255 characters in the format defined by RFC 822, such as `sec@abc.com`.
- **key-id** *key-id-string*: Uses the peer's key ID as the peer ID for IKEv2 profile matching. The *key-id-string* argument is a case-sensitive string of 1 to 255 characters, and is usually a vendor-specific string for doing proprietary types of identification.

Usage guidelines

The device compares the received peer ID with the peer IDs configured in local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. If you have configured the **match local address** and **match vrf** commands, the IKEv2 profile must also match the specified local interface or address and the specified VPN instance.

To make sure only one IKEv2 profile is matched for a peer, do not configure the same peer ID for two or more IKEv2 profiles. If you configure the same peer ID for two or more IKEv2 profiles, which IKEv2 profile is selected for IKEv2 negotiation is unpredictable.

You can configure an IKEv2 profile to match multiple peer IDs. A peer ID configured earlier has a higher priority.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

Configure the IKEv2 profile to match the peer ID that is the FQDN name `www.test.com`.

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

Configure the IKEv2 profile to match the peer ID that is the IP address `10.1.1.1`.

```
[Sysname-ikev2-profile-profile1] match remote identity address 10.1.1.1
```

Related commands

- **identity local**
- **match local address**
- **match vrf**

New command: match vrf (IKEv2 policy view)

Use **match vrf** to specify a VPN instance that an IKEv2 policy matches.

Use **undo match vrf** to restore the default.

Syntax

```
match vrf { name vrf-name | any }
```

```
undo match vrf
```

Default

No VPN instance is specified, and the IKEv2 policy matches all local IP addresses in the public network.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

name *vrf-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

any: Specifies the public network and all VPN instances.

Usage guidelines

Each end must have an IKEv2 policy for the IKE_SA_INIT exchange. The initiator looks up an IKEv2 policy by the IP address of the interface to which the IPsec policy is applied and the VPN instance to which the interface belongs. The responder looks up an IKEv2 policy by the IP address of the interface that receives the IKEv2 packet and the VPN instance to which the interface belongs.

IKEv2 policies with this command configured are looked up before those that do not have this command configured.

Examples

Create an IKEv2 policy named **policy1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 policy policy1
```

Configure the IKEv2 policy to match the VPN instance **vpn1**.

```
[Sysname-ikev2-policy-policy1] match vrf name vpn1
```

Related commands

- **display ikev2 policy**
- **match local address**

New command: match vrf (IKEv2 profile view)

Use **match vrf** to specify a VPN instance for an IKEv2 profile.

Use **undo match vrf** to restore the default.

Syntax

match vrf { **name** *vrf-name* | **any** }

undo match vrf

Default

An IKEv2 profile belongs to the public network.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

name *vrf-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

any: Specifies the public network and all VPN instances.

Usage guidelines

If an IKEv2 profile belongs to a VPN instance, only interfaces in the VPN instance can use the IKEv2 profile for IKEv2 negotiation. The VPN instance is the VPN instance to which the interface that receives IKEv2 packets belongs. If you specify the **any** keyword, interfaces in any VPN instance can use the IKEv2 profile for IKEv2 negotiation.

Examples

```
# Create an IKEv2 profile named profile1.
<Sysname> system-view
[Sysname] ikev2 profile profile1

# Specify vrf1 as the VPN instance that the IKEv2 profile belongs to.
[Sysname-ikev2-profile-profile1] match vrf name vrf1
```

Related commands

match remote

New command: nat-keepalive

Use **nat-keepalive** to set the NAT keepalive interval.

Use **ikev2 nat-keepalive** to restore the default.

Syntax

nat-keepalive *seconds*

undo nat-keepalive

Default

The NAT keepalive interval set in system view is used.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the NAT keepalive interval in seconds, in the range of 5 to 3600.

Usage guidelines

This command takes effect when the device resides in the private network behind a NAT device. The device must send NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

Examples

```
# Create an IKEv2 profile named profile1.
<Sysname> system-view
[Sysname] ikev2 profile profile1

# Set the NAT keepalive interval to 1200 seconds.
[Sysname-ikev2-profile-profile1] nat-keepalive 1200
```

Related commands

- **display ikev2 profile**
- **ikev2 nat-keepalive**

New command: peer

Use **peer** to create an IKEv2 peer and enter its view, or enter the view of an existing IKEv2 peer.

Use **undo peer** to delete an IKEv2 peer.

Syntax

peer *name*

undo peer *name*

Default

No IKEv2 peers exist.

Views

IKEv2 keychain view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the IKEv2 peer. The peer name is a case-insensitive string of 1 to 63 characters.

Usage guidelines

An IKEv2 peer contains a pre-shared key and the criteria for looking up the peer. The criteria for peer lookup include the peer's host name, IP address, IP address range, and ID. The IKEv2 negotiation initiator uses the peer's host name, IP address, or IP address range to look up its peer. The responder uses the peer's IP address, IP address range, or ID to look up its peer.

Examples

Create an IKEv2 keychain named **key1** and enter IKEv2 keychain view.

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Related commands

- **address**
- **hostname**
- **identity**
- **ikev2 keychain**

New command: pre-shared-key

Use **pre-shared-key** to configure a pre-shared key.

Use **undo pre-shared-key** to delete a pre-shared key.

Syntax

pre-shared-key [**local** | **remote**] { **ciphertext** | **plaintext** } *string*

undo pre-shared-key [**local** | **remote**]

Default

No pre-shared key exists.

Views

IKEv2 peer view

Predefined user roles

network-admin

Parameters

local: Specifies a pre-shared key for certificate signing.

remote: Specifies a pre-shared key for certificate authentication.

ciphertext: Specifies a pre-shared key in encrypted form.

plaintext: Specifies a pre-shared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the pre-shared key. The key is case sensitive. In non-FIPS mode, its plaintext form is a string of 1 to 128 characters and its encrypted form is a string of 1 to 201 characters. In FIPS mode, its plaintext form is a string of 15 to 128 characters and its encrypted form is a string of 15 to 201 characters.

Usage guidelines

If you specify the **local** or **remote** keyword, you configure an asymmetric key. If you specify neither the **local** nor the **remote** keyword, you configure a symmetric key.

To delete a key by using the **undo** command, you must specify the correct key type. For example, if you configure a key by using the **pre-shared-key local** command, you cannot delete the key by using the **undo pre-shared-key** or **undo pre-shared-key remote** command.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

- On the initiator:

Create an IKEv2 keychain named **key1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain key1
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-key1] peer peer1
```

Configure the symmetric plaintext pre-shared key **111-key**.

```
[Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
```

```
[Sysname-ikev2-keychain-key1-peer-peer1] quit
```

Create an IKEv2 peer named **peer2**.

```
[Sysname-ikev2-keychain-key1] peer peer2
```

Configure asymmetric plaintext pre-shared keys. The key for certificate signing is **111-key-a** and the key for certificate authentication is **111-key-b**.

```
[Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key local plaintext 111-key-a
```

```
[Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key remote plaintext 111-key-b
```

- On the responder:

Create an IKEv2 keychain named **telecom**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain telecom
```

Create an IKEv2 peer named **peer1**.

```
[Sysname-ikev2-keychain-telecom] peer peer1
```

Configure the symmetric plaintext pre-shared key **111-key**.

```
[Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
```

```
[Sysname-ikev2-keychain-telecom-peer-peer1] quit
```

Create an IKEv2 peer named **peer2**.

```
[Sysname-ikev2-keychain-telecom] peer peer2
# Configure asymmetric plaintext pre-shared keys. The key for certificate signing is 111-key-b
and the key for certificate authentication is 111-key-a.
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key local plaintext
111-key-b
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key remote plaintext
111-key-a
```

Related commands

- **ikev2 keychain**
- **peer**

New command: prf

Use **prf** to specify pseudo-random function (PRF) algorithms for an IKEv2 proposal.

Use **undo prf** to restore the default.

Syntax

In non-FIPS mode:

```
prf { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 } *
```

```
undo prf
```

In FIPS mode:

```
prf { sha1 | sha256 | sha384 | sha512 } *
```

```
undo prf
```

Default

An IKEv2 proposal uses the integrity protection algorithms as the PRF algorithms.

Views

IKEv2 proposal view

Predefined user roles

network-admin

Parameters

aes-xcbc-mac: Uses the HMAC-AES-XCBC-MAC algorithm.

md5: Uses the HMAC-MD5 algorithm.

sha1: Uses the HMAC-SHA1 algorithm.

sha256: Uses the HMAC-SHA256 algorithm.

sha384: Uses the HMAC-SHA384 algorithm.

sha512: Uses the HMAC-SHA512 algorithm.

Usage guidelines

You can specify multiple PRF algorithms for an IKEv2 proposal. An algorithm specified earlier has a higher priority.

Examples

Create an IKEv2 proposal named **prop1**.

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
```

```
# Specify HMAC-SHA1 and HMAC-MD5 as the PRF algorithms, with HMAC-SHA1 preferred.  
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

Related commands

- **ikev2 proposal**
- **integrity**

New command: priority (IKEv2 policy view)

Use **priority** to set a priority for an IKEv2 policy.

Use **undo priority** to restore the default.

Syntax

```
priority priority  
undo priority
```

Default

The priority of an IKEv2 policy is 100.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

priority: Specifies the priority of the IKEv2 policy, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 policies.

Examples

```
# Set the priority to 10 for the IKEv2 policy policy1.
```

```
<Sysname> system-view  
[Sysname] ikev2 policy policy1  
[Sysname-ikev2-policy-policy1] priority 10
```

Related commands

```
display ikev2 policy
```

New command: priority (IKEv2 profile view)

Use **priority** to set a priority for an IKEv2 profile.

Use **undo priority** to restore the default.

Syntax

```
priority priority  
undo priority
```

Default

The priority of an IKEv2 profile is 100.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

priority: Specifies the priority of the IKEv2 profile, in the range of 1 to 65535. A smaller number represents a higher priority.

Usage guidelines

The priority set by this command can only be used to adjust the match order of IKEv2 profiles.

Examples

```
# Set the priority to 10 for the IKEv2 profile profile1.
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] priority 10
```

New command: proposal

Use **proposal** to specify an IKEv2 proposal for an IKEv2 policy.

Use **undo proposal** to remove an IKEv2 proposal from an IKEv2 policy.

Syntax

```
proposal proposal-name
undo proposal proposal-name
```

Default

No IKEv2 proposal is specified for an IKEv2 policy.

Views

IKEv2 policy view

Predefined user roles

network-admin

Parameters

proposal-name: Specifies an IKEv2 proposal by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

Examples

```
# Specify the IKEv2 proposal proposal1 for the IKEv2 policy policy1.
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] proposal proposal1
```

Related commands

- **display ikev2 policy**
- **ikev2 proposal**

New command: reset ikev2 sa

Use **reset ikev2 sa** to delete IKEv2 SAs.

Syntax

```
reset ikev2 sa [ [ { local | remote } { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] ] | tunnel tunnel-id ] [ fast ]
```

Views

User view

Predefined user roles

network-admin

Parameters

local: Deletes IKEv2 SAs for a local IP address.

remote: Deletes IKEv2 SAs for a remote IP address.

ipv4-address: Specifies a local or remote IPv4 address.

ipv6 *ipv6-address*: Specifies a local or remote IPv6 address.

vpn-instance *vpn-instance-name*: Deletes IKEv2 SAs in an MPLS L3VPN instance. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command deletes IKEv2 SAs for the public network.

tunnel *tunnel-id*: Deletes IKEv2 SAs for an IPsec tunnel. The *tunnel-id* argument specifies an IPsec tunnel by its ID in the range of 1 to 2000000000.

fast: Notifies the peers of the deletion and deletes IKEv2 SAs directly before receiving the peers' responses. If you do not specify this keyword, the device notifies the peers of the deletion and deletes IKEv2 SAs after it receives the peers' responses.

Usage guidelines

Deleting an IKEv2 SA will also delete the child SAs negotiated through the IKEv2 SA.

If you do not specify any parameters, this command deletes all IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.

Examples

Display information about IKEv2 SAs.

```
<Sysname> display ikev2 sa
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	1.1.1.2/500	EST
2	2.2.2.1/500	2.2.2.2/500	EST

Status:

IN-NEGO: Negotiating EST: Established, DEL: Deleting

Delete the IKEv2 SA whose remote IP address is 1.1.1.2.

```
<Sysname> reset ikev2 sa remote 1.1.1.2
```

Display information about IKEv2 SAs again. Verify that the IKEv2 SA is deleted.

```
<Sysname> display ikev2 sa
```

Tunnel ID	Local	Remote	Status
2	2.2.2.1/500	2.2.2.2/500	EST

Status:

IN-NEGO: Negotiating EST: Established, DEL: Deleting

Related commands

display ikev2 sa

New command: reset ikev2 statistics

Use **reset ikev2 statistics** to clear IKEv2 statistics.

Syntax

reset ikev2 statistics

Views

Any view

Predefined user roles

network-admin

Examples

Clear IKEv2 statistics.

```
<Sysname> reset ikev2 statistics
```

New command: sa duration

Use **sa duration** to set the IKEv2 SA lifetime.

Use **undo sa duration** to restore the default.

Syntax

sa duration *seconds*

undo sa duration

Default

The IKEv2 SA lifetime is 86400 seconds.

Views

IKEv2 profile view

Predefined user roles

network-admin

Parameters

seconds: Specifies the IKEv2 SA lifetime in seconds, in the range of 120 to 86400.

Usage guidelines

An IKEv2 SA can be used for subsequent IKEv2 negotiations before its lifetime expires, saving a lot of negotiation time. However, the longer the lifetime, the higher the possibility that attackers collect enough information and initiate attacks.

Two peers can have different IKEv2 SA lifetime settings, and they do not perform lifetime negotiation. The peer with a shorter lifetime always initiates the rekeying.

Examples

Create an IKEv2 profile named **profile1**.

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
# Set the IKEv2 SA lifetime to 1200 seconds.
[Sysname-ikev2-profile-profile1] sa duration 1200
```

Related commands

display ikev2 profile

New command: esn enable

Use **esn enable** to enable the Extended Sequence Number (ESN) feature.

Use **undo esn enable** to disable the ESN feature.

Syntax

esn enable [both]

undo esn enable

Default

ESN is disabled.

Views

IPsec transform set view

Predefined user roles

network-admin

Parameters

both: Specifies IPsec to support both extended sequence number and traditional sequence number. If you do not specify this keyword, IPsec only supports extended sequence number.

Usage guidelines

The ESN feature extends the sequence number length from 32 bits to 64 bits. This feature prevents the sequence number space from being exhausted when large volumes of data are transmitted at high speeds over an IPsec SA. If the sequence number space is not exhausted, the IPsec SA does not need to be renegotiated.

This feature must be enabled at both the initiator and the responder.

Examples

Enable the ESN feature in the IPsec transform set **tran1**.

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esn enable
```

Related commands

display ipsec transform-set

New command: ikev2-profile

Use **ikev2-profile** to specify an IKEv2 profile for an IPsec policy or IPsec policy template.

Use **undo ikev2-profile** to restore the default.

Syntax

ikev2-profile *profile-name*

undo ikev2-profile

Default

No IKEv2 profile is specified.

Views

IPsec policy view, IPsec policy template view

Predefined user roles

network-admin

Parameters

profile-name: Specifies an IKEv2 profile by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

The IKEv2 profile specified for an IPsec policy or IPsec policy template defines the parameters used for IKEv2 negotiation.

You can specify only one IKEv2 profile for an IPsec policy or IPsec policy template. On the initiator, an IKEv2 profile is required. On the responder, an IKEv2 profile is optional. If you do not specify an IKEv2 profile, the responder can use any IKEv2 profile for negotiation.

Examples

Specify the IKEv2 profile **profile1** for the IPsec policy **policy1**.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ikev2-profile profile1
```

Related commands

- **display ipsec ipv6-policy**
- **display ipsec policy**
- **ikev2 profile**

New command: tfc enable

Use **tfc enable** to enable the Traffic Flow Confidentiality (TFC) padding feature.

Use **undo tfc enable** to disable the TFC padding feature.

Syntax

tfc enable

undo tfc enable

Default

TFC padding is disabled.

Views

IPsec policy view, IPsec policy template view

Predefined user roles

network-admin

Usage guidelines

The TFC padding feature can hide the length of the original packet, and might affect the packet encapsulation and de-encapsulation performance. This feature takes effect on UDP packets

encapsulated by ESP in transport mode and on original IP packets encapsulated by ESP in tunnel mode.

Examples

```
# Enable TFC padding for the IPsec policy policy1.
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] tfc enable
```

Related commands

- **display ipsec ipv6-policy**
- **display ipsec policy**

Modified command: ah authentication-algorithm

Old syntax

In non-FIPS mode:

```
ah authentication-algorithm { md5 | sha1 | sm3 } *
```

```
undo ah authentication-algorithm
```

In FIPS mode:

```
ah authentication-algorithm sha1
```

```
undo ah authentication-algorithm
```

New syntax

In non-FIPS mode:

```
ah authentication-algorithm { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 | sm3 } *
```

```
undo ah authentication-algorithm
```

In FIPS mode:

```
ah authentication-algorithm { sha1 | sha256 | sha384 | sha512 } *
```

```
undo ah authentication-algorithm
```

Views

IPsec transform set view

Change description

The following keywords were added:

- **aes-xcbc-mac**: Specifies the HMAC-AES-XCBC-MAC algorithm.
- **sha256**: Specifies the HMAC-SHA256 algorithm.
- **sha384**: Specifies the HMAC-SHA384 algorithm.
- **sha512**: Specifies the HMAC-SHA512 algorithm.

Modified command: display ipsec { ipv6-policy | policy }

Syntax

```
display ipsec { ipv6-policy | policy } [ policy-name [ seq-number ] ]
```

Views

Any view

Change description

The following fields were added to the command output:

- **Traffic Flow Confidentiality**—Whether Traffic Flow Confidentiality (TFC) padding is enabled.
- **IKEv2 profile**—IKEv2 profile used by the IPsec policy.

Modified command: display ipsec { ipv6-policy-template | policy-template }

Syntax

```
display ipsec { ipv6-policy-template | policy-template } [ template-name [ seq-number ] ]
```

Views

Any view

Change description

The following fields were added to the command output:

- **Traffic Flow Confidentiality**—Whether Traffic Flow Confidentiality (TFC) padding is enabled.
- **Selector mode**—Data flow protection mode of the IPsec policy template.
- **Local address**—Local end IP address of the IPsec tunnel.
- **IKEv2 profile**—IKEv2 profile used by the IPsec policy template.
- **SA idle time**—Idle timeout of the IPsec SA, in seconds.

Modified command: display ipsec sa

Syntax

```
display ipsec sa [ brief | count | interface interface-type interface-number | { ipv6-policy | policy } policy-name [ seq-number ] | profile profile-name | remote [ ipv6 ] ip-address ]
```

Views

Any view

Change description

The following fields were added to the command output:

- **Extended Sequence Number enable**—Whether Extended Sequence Number (ESN) is enabled.
- **Traffic Flow Confidentiality enable**—Whether Traffic Flow Confidentiality (TFC) padding is enabled.
- **Inside VRF**—VPN instance to which the protected data flow belongs.

The following values were added to the **Perfect Forward Secrecy** field:

- **dh-group19**—256-bit ECP Diffie-Hellman group.
- **dh-group20**—384-bit ECP Diffie-Hellman group.

Modified command: display ipsec transform-set

Syntax

```
display ipsec transform-set [ transform-set-name ]
```

Views

Any view

Change description

The following fields were added to the command output:

- **ESN**—Whether Extended Sequence Number (ESN) is enabled.
- **PFS**—Perfect Forward Secrecy (PFS) configuration.

Modified command: display ipsec tunnel

Syntax

```
display ipsec tunnel { brief | count | tunnel-id tunnel-id }
```

Views

Any view

Change description

The following values were added to the **Perfect Forward Secrecy** field of the command output:

- **dh-group19**—256-bit ECP Diffie-Hellman group.
- **dh-group20**—384-bit ECP Diffie-Hellman group.

Modified command: esp authentication-algorithm

Old syntax

In non-FIPS mode:

```
esp authentication-algorithm { md5 | sha1 | sm3 } *  
undo esp authentication-algorithm
```

In FIPS mode:

```
esp authentication-algorithm sha1  
undo esp authentication-algorithm
```

New syntax

In non-FIPS mode:

```
esp authentication-algorithm { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 | sm3 } *  
undo esp authentication-algorithm
```

In FIPS mode:

```
esp authentication-algorithm { sha1 | sha256 | sha384 | sha512 } *  
undo esp authentication-algorithm
```

Views

IPsec transform set view

Change description

The following keywords were added:

- **aes-xcbc-mac**: Specifies the HMAC-AES-XCBC-MAC algorithm.
- **sha256**: Specifies the HMAC-SHA256 algorithm.
- **sha384**: Specifies the HMAC-SHA384 algorithm.

- **sha512**: Specifies the HMAC-SHA512 algorithm.

Modified command: esp encryption-algorithm

Old syntax

In non-FIPS mode:

```
esp encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des-cbc | null }
*
```

```
undo esp encryption-algorithm
```

In FIPS mode:

```
esp encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 }*
```

```
undo esp encryption-algorithm
```

New syntax

In non-FIPS mode:

```
esp encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-ctr-128 |
aes-ctr-192 | aes-ctr-256 | camellia-cbc-128 | camellia-cbc-192 | camellia-cbc-256 | des-cbc |
gmac-128 | gmac-192 | gmac-256 | gcm-128 | gcm-192 | gcm-256 | null }*
```

```
undo esp encryption-algorithm
```

In FIPS mode:

```
esp encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-ctr-128 | aes-ctr-192
| aes-ctr-256 | gmac-128 | gmac-192 | gmac-256 | gcm-128 | gcm-192 | gcm-256 }*
```

```
undo esp encryption-algorithm
```

Views

IPsec transform set view

Change description

The following keywords were added:

- **aes-ctr-128**: Uses the AES algorithm with a 128-bit key in CTR mode. This keyword is available only for IKEv2.
- **aes-ctr-192**: Uses the AES algorithm with a 192-bit key in CTR mode. This keyword is available only for IKEv2.
- **aes-ctr-256**: Uses the AES algorithm with a 256-bit key in CTR mode. This keyword is available only for IKEv2.
- **camellia-cbc-128**: Uses the Camellia algorithm with a 128-bit key in CBC mode. This keyword is available only for IKEv2.
- **camellia-cbc-192**: Uses the Camellia algorithm with a 192-bit key in CBC mode. This keyword is available only for IKEv2.
- **camellia-cbc-256**: Uses the Camellia algorithm with a 256-bit key in CBC mode. This keyword is available only for IKEv2.
- **gmac-128**: Uses the GMAC algorithm with a 128-bit key. This keyword is available only for IKEv2.
- **gmac-192**: Uses the GMAC algorithm with a 192-bit key. This keyword is available only for IKEv2.
- **gmac-256**: Uses the GMAC algorithm with a 256-bit key. This keyword is available only for IKEv2.
- **gcm-128**: Uses the GCM algorithm with a 128-bit key. This keyword is available only for IKEv2.

- **gcm-192**: Uses the GCM algorithm with a 192-bit key. This keyword is available only for IKEv2.
- **gcm-256**: Uses the GCM algorithm with a 256-bit key. This keyword is available only for IKEv2.

Modified command: pfs

Old syntax

In non-FIPS mode:

```
pfs { dh-group1 | dh-group2 | dh-group5 | dh-group14 | dh-group24 }
```

```
undo pfs
```

In FIPS mode:

```
pfs dh-group14
```

```
undo pfs
```

New syntax

In non-FIPS mode:

```
pfs { dh-group1 | dh-group2 | dh-group5 | dh-group14 | dh-group19 | dh-group20 | dh-group24 }
```

```
undo pfs
```

In FIPS mode:

```
pfs { dh-group14 | dh-group19 | dh-group20 | dh-group24 }
```

```
undo pfs
```

Views

IPsec transform set view

Change description

The following keywords were added:

- **dh-group19**: Uses 256-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.
- **dh-group20**: Uses 384-bit ECP Diffie-Hellman group. This keyword is available only for IKEv2.

Modified command: pre-shared-key

Old syntax

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key { cipher cipher-key | simple simple-key }
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

New syntax

In non-FIPS mode:

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key { cipher cipher-key | simple simple-key }
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

In FIPS mode:

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key [ cipher cipher-key ]
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

Views

IKE keychain view

Change description

After modification, if you do not specify the **cipher** *cipher-key* option, you specify a plaintext pre-shared key in interactive mode. The key is a case-sensitive string of 15 to 128 characters, and it must contain uppercase and lowercase letters, digits, and special characters other than the question mark (?). In non-FIPS mode, this command does not support configuring a pre-shared key in interactive mode.

Modified command: authentication-algorithm

Old syntax

In non-FIPS mode:

```
authentication-algorithm { md5 | sha | sm3 }
```

```
undo authentication-algorithm
```

In FIPS mode:

```
authentication-algorithm sha
```

```
undo authentication-algorithm
```

New syntax

In non-FIPS mode:

```
authentication-algorithm { md5 | sha | sha256 | sha384 | sha512 | sm3 }
```

```
undo authentication-algorithm
```

In FIPS mode:

```
authentication-algorithm { sha | sha256 | sha384 | sha512 }
```

```
undo authentication-algorithm
```

Views

IKE proposal view

Change description

The following keywords were added:

- **sha256**: Specifies the HMAC-SHA256 algorithm.
- **sha384**: Specifies the HMAC-SHA384 algorithm.
- **sha512**: Specifies the HMAC-SHA512 algorithm.

-

New feature: SSL support for Suite B

Configuring Suite B in SSL

Suite B contains a set of encryption and authentication algorithms that meet high security requirements.

In this software version, Suite B is available in SSL. In addition, a new command was added to display the algorithm version number on the device.

Command reference

New command: display crypto version

Use **display crypto version** to display the algorithm version number.

Syntax

display crypto version

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The algorithm version number identifies a suite of cryptographic algorithms.

Examples

Display the algorithm version number.

```
<Sysname> display crypto version
```

```
7.1.1.886
```

Table 6 Command output

Field	Description
7.1.1.886	Version number information, in the format of 7.1.X. 7.1 represents Comware V700R001, and X represents the algorithm version number.

New command: ssl version disable

Use **ssl version disable** to disable SSL protocol versions on the device.

Use **undo ssl version disable** enable SSL protocol versions on the device.

Syntax

In non-FIPS mode:

ssl version { ssl3.0 | tls1.0 | tls1.1 } * disable

undo ssl version { ssl3.0 | tls1.0 | tls1.1 } * disable

In FIPS mode:

ssl version { tls1.0 | tls1.1 } * disable

undo ssl version { tls1.0 | tls1.1 } * disable

Default

In non-FIPS mode, the device supports SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.

In FIPS mode, the device supports TLS 1.0, TLS 1.1, and TLS 1.2.

Views

System view

Predefined user roles

network-admin

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

tls1.1: Specifies TLS 1.1.

Usage guidelines

Use this command to disable SSL 3.0, TLS 1.0, and TLS 1.1 on the device to enhance system security.

- An SSL client always uses the SSL protocol version specified for it (by using the **version** command), whether you disable the SSL protocol version or not.
- An SSL server supports only TLS 1.2 after SSL 3.0, TLS 1.0, and TLS 1.1 are disabled.

Disabling an SSL protocol version on the device does not affect the availability of earlier SSL protocol versions. For example, if you execute the **ssl version tls1.1 disable** command, TLS 1.1 is disabled but TLS 1.0 is still available.

In FIPS mode, the device does not support SSL 3.0.

Examples

Disable SSL 3.0 on the device.

```
<Sysname> system-view
```

```
[Sysname] ssl version ssl3.0 disable
```

Disable TLS 1.0 on the device.

```
<Sysname> system-view
```

```
[Sysname] ssl version tls1.0 disable
```

New command: ssl renegotiation disable

Use **ssl renegotiation disable** to disable SSL session renegotiation.

Use **undo ssl renegotiation disable** to restore the default.

Syntax

ssl renegotiation disable

undo ssl renegotiation disable

Default

SSL session renegotiation is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The SSL session renegotiation feature enables the SSL client and server to reuse a previously negotiated SSL session for an abbreviated handshake.

Disabling session renegotiation causes more computational overhead to the system but it can avoid potential risks. Disable SSL session renegotiation only when explicitly required.

Examples

```
# Disable SSL session renegotiation.  
<Sysname> system-view  
[Sysname] ssl renegotiation disable
```

Modified command: version

Old syntax

In non-FIPS mode:

version { ssl3.0 | tls1.0 }

undo version

In FIPS mode:

version tls1.0

undo version

New syntax

In non-FIPS mode:

version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 }

undo version

In FIPS mode:

version { tls1.0 | tls1.1 | tls1.2 }

undo version

Views

SSL client policy view

Change description

The following keywords were added:

- **tls1.1**: Specifies TLS 1.0 for the SSL client policy.
- **tls1.2**: Specifies TLS 1.2 for the SSL client policy.

Modified command: ciphersuite

Old syntax

In non-FIPS mode:

```
ciphersuite {    dhe_rsa_aes_128_cbc_sha    |    dhe_rsa_aes_256_cbc_sha    |
exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_edc_cbc_sha |
rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 |
rsa_rc4_128_sha } *
```

undo ciphersuite

In FIPS mode:

```
ciphersuite { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha
| rsa_aes_256_cbc_sha } *
```

undo ciphersuite

New syntax

In non-FIPS mode:

```
ciphersuite {    dhe_rsa_aes_128_cbc_sha    |    dhe_rsa_aes_256_cbc_sha    |
exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_edc_cbc_sha |
rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 |
rsa_rc4_128_sha    |    rsa_aes_128_cbc_sha256    |    rsa_aes_256_cbc_sha256    |
dhe_rsa_aes_128_cbc_sha256    |    dhe_rsa_aes_256_cbc_sha256    |
ecdhe_rsa_aes_128_cbc_sha256    |    ecdhe_rsa_aes_256_cbc_sha384    |
ecdhe_rsa_aes_128_gcm_sha256    |    ecdhe_rsa_aes_256_gcm_sha384    |
ecdhe_ecdsa_aes_128_cbc_sha256    |    ecdhe_ecdsa_aes_256_cbc_sha384    |
ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_gcm_sha384 } *
```

undo ciphersuite

In FIPS mode:

```
cipher { rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha256 |
rsa_aes_256_cbc_sha256 | ecdhe_rsa_aes_128_cbc_sha256 |
ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_128_gcm_sha256 |
ecdhe_rsa_aes_256_gcm_sha384 | ecdhe_ecdsa_aes_128_cbc_sha256 |
ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_128_gcm_sha256 |
ecdhe_ecdsa_aes_256_gcm_sha384 } *
```

undo ciphersuite

Views

SSL server policy view

Change description

The following keywords were added:

- **rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 128-bit AES CBC , and the MAC algorithm SHA256.
- **rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_rsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.

- **ecdhe_rsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.

Modified command: prefer-cipher

Old syntax

In non-FIPS mode:

```
prefer-cipher {   dhe_rsa_aes_128_cbc_sha   |   dhe_rsa_aes_256_cbc_sha   |
exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_edc_cbc_sha |
rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 |
rsa_rc4_128_sha }
```

undo prefer-cipher

In FIPS mode:

```
prefer-cipher {   dhe_rsa_aes_128_cbc_sha   |   dhe_rsa_aes_256_cbc_sha   |
rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha }
```

undo prefer-cipher

New syntax

In non-FIPS mode:

```
prefer-cipher {   dhe_rsa_aes_128_cbc_sha   |   dhe_rsa_aes_256_cbc_sha   |
exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_edc_cbc_sha |
rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 |
rsa_rc4_128_sha   |   rsa_aes_128_cbc_sha256   |   rsa_aes_256_cbc_sha256   |
dhe_rsa_aes_128_cbc_sha256   |   dhe_rsa_aes_256_cbc_sha256   |
ecdhe_rsa_aes_128_cbc_sha256   |   ecdhe_rsa_aes_256_cbc_sha384   |
ecdhe_rsa_aes_128_gcm_sha256   |   ecdhe_rsa_aes_256_gcm_sha384   |
ecdhe_ecdsa_aes_128_cbc_sha256   |   ecdhe_ecdsa_aes_256_cbc_sha384   |
ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_gcm_sha384 }
```

undo prefer-cipher

In FIPS mode:

```
prefer-cipher { rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha256 |
rsa_aes_256_cbc_sha256 | ecdhe_rsa_aes_128_cbc_sha256 |
ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_128_gcm_sha256 |
ecdhe_rsa_aes_256_gcm_sha384 | ecdhe_ecdsa_aes_128_cbc_sha256 |
ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_128_gcm_sha256 |
ecdhe_ecdsa_aes_256_gcm_sha384 }
```

undo prefer-cipher

Views

SSL client policy view

Change description

The following keywords were added:

- **rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 128-bit AES CBC , and the MAC algorithm SHA256.
- **rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **dhe_rsa_aes_256_cbc_sha256**: Specifies the key exchange algorithm DHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_rsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_rsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE RSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_cbc_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES CBC, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_cbc_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES CBC, and the MAC algorithm SHA384.
- **ecdhe_ecdsa_aes_128_gcm_sha256**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 128-bit AES GCM, and the MAC algorithm SHA256.
- **ecdhe_ecdsa_aes_256_gcm_sha384**: Specifies the key exchange algorithm ECDHE ECDSA, the data encryption algorithm 256-bit AES GCM, and the MAC algorithm SHA384.

New feature: FIPS support for Suit B

Configuring Suite B in FIPS

Suite B contains a set of encryption and authentication algorithms that meet high security requirements.

In this software version, new FIPS commands were added to support Suite B.

Command reference

New command: fips rng random size filename

Use **fips rng random size filename** to generate a random number and save it to a file.

Syntax

fips rng random size *random-size* **filename** *filename*

Views

Probe view

Predefined user roles

network-admin

Parameters

random-size: Specifies the random number size in the range of 1 to 1000000 bytes.

filename: Specifies the name of the file to save the random number. The file name is a case-insensitive string.

Usage guidelines

Use this command in FIPS mode to generate a random number and save it to a file.

Examples

Generate a 100000-byte random number and save it to a file named **out.bin**.

```
<Sysname> system-view
```

```
[Sysname-probe] fips rng random size 100000 filename out.bin
```

```
Generating random number. Please wait...
```

```
Random number saved to file successfully.
```

New command: fips rng random size round rate-statistics

Use **fips rng random size round rate-statistics** to calculate the average rate at which random numbers are generated.

Syntax

fips rng random size *random-size* **round** *round* **rate-statistics**

Views

Probe view

Predefined user roles

network-admin

Parameters

random-size: Specifies the random number size in the range of 1 to 1000000 bytes.

round: Specifies the number of random number generations, in the range of 3 to 10.

Usage guidelines

Use this command in FIPS mode to calculate the average rate at which random numbers are generated.

Examples

Generate five 100000-byte random numbers and calculate the average rate at which the random numbers are generated.

```
<Sysname> system-view
```

```
[Sysname-probe] fips rng random size 100000 round 5 rate-statistics
```

```
Random number generated successfully.
```

```
Rate: 5000 bytes/s
```

```
Rate: 5100 bytes/s
```

```
Rate: 4900 bytes/s
```

```
Rate: 4800 bytes/s
```

```
Rate: 52000 bytes/s
```

```
Average rate: 5000 bytes/s
```

New command: **fips rng entropy size filename**

Use **fips rng entropy size filename** to generate a random number entropy and save it to a file.

Syntax

fips rng entropy size *entropy-size filename filename*

Views

Probe view

Predefined user roles

network-admin

Parameters

entropy-size: Specifies the random number entropy size in the range of 1 to 1000000 bytes.

filename: Specifies the name of the file to save the random number entropy. The file name is a case-insensitive string.

Usage guidelines

Use this command in FIPS mode to generate a random number entropy and save it to a file.

Examples

Generate a 100000-byte random number entropy and save it to a file named **out.bin**.

```
<Sysname> system-view
```

```
[Sysname-probe] fips rng entropy size 100000 filename out.bin
```

```
Generating random number entropy. Please wait...
```

```
Entropy saved to file successfully.
```

New command: **fips rng entropy size round rate-statistics**

Use **fips rng entropy size round rate-statistics** to calculate the average rate at which random number entropies are generated.

Syntax

fips rng entropy size *entropy-size round round rate-statistics*

Views

Probe view

Predefined user roles

network-admin

Parameters

entropy-size: Specifies the random number entropy size in the range of 1 to 1000000 bytes.

round: Specifies the number of random number entropy generations, in the range of 3 to 10.

Usage guidelines

Use this command in FIPS mode to calculate the average rate at which random number entropies are generated.

Examples

Generate five 100000-byte random number entropies and calculate the average rate at which the random number entropies are generated.

```
<Sysname> system-view
```

```
[Sysname-probe]fips rng entropy size 100000 round 5 rate-statistics
Entropy generated successfully.
Rate: 5000 bytes/s
Rate: 5100 bytes/s
Rate: 4900 bytes/s
Rate: 4800 bytes/s
Rate: 52000 bytes/s
Average rate: 5000 bytes/s
```

New command: fips kdf

Use **fips kdf** to derive a key from an import file and save it to an export file.

Syntax

```
fips kdf { ikev1 { dsa | psk } | ikev2 | tls } import inputfile export outputfile
```

Views

Probe view

Predefined user roles

network-admin

Usage guidelines

Use this command in FIPS mode to derive a key for the third-party to determine whether the key meets the CC/FIPS authentication requirements.

Examples

```
# Derive an ikev1 pre-shared key from an import file named ikev1_psk.req and save the key to an
export file named ikev1_psk.rsp.
<Sysname> system-view
[Sysname-probe] fips kdf ikev1 psk import ikev1_psk.req export ikev1_psk.rsp
```

New command: fips algorithm verify

Use **fips algorithm verify** to execute an algorithm test vector and generate a result file.

Syntax

```
fips algorithm verify param
```

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command in FIPS mode to execute an algorithm test vector and generate a result file for the third-party to verify the result.

Examples

```
# Execute the DSA2 test vector in a file named 01-HP-MPC8544/DSA2/req/PQGGen.req, and
generate a result file named 01-HP-MPC8544/DSA2/resp/PQGGen.rsp.
<Sysname> system-view
```

```
[Sysname] fips algorithm verify fips_dssvs pqq 01-HP-MPC8544/DSA2/req/PQGGen.req
01-HP-MPC8544/DSA2/resp/PQGGen.rsp
```

Modified command: fips self-test

Syntax

fips self-test

Views

System view

Change description

Self-tests were added for the following algorithms:

- 3DES.
- ECDH.
- GCM.
- GMAC.
- Random number generator (RNG).

New feature: SSH support for Suite B

Configuring SSH based on Suite B algorithms

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. [Table 7](#) lists all algorithms in Suite B.

The SSH server and client support using the X.509v3 certificate for identity authentication in compliance with the algorithm, negotiation, and authentication specifications defined in RFC 6239.

Table 7 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AEAD_AES_128_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256 ecdh-sha2-nistp384	AEAD_AES_128_GCM AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

Specifying a PKI domain for the SSH server

The PKI domain specified for the SSH server has the following functions:

- The SSH server uses the PKI domain to send its certificate to the client in the key exchange stage.
- The SSH server uses the PKI domain to authenticate the client's certificate if no PKI domain is specified for the client authentication by using the **ssh user** command.

To specify a PKI domain for the SSH server:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify a PKI domain for the SSH server.	ssh server pki-domain <i>domain-name</i>	By default, no PKI domain is specified for the SSH server.

Establishing a connection to an Stelnet server based on Suite B

Task	Command	Remarks
Establish a connection to an Stelnet server based on Suite B.	- Establish a connection to an IPv4 Stelnet server based on Suite B: ssh2 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [prefer-compress zlib] [dscp <i>dscp-value</i> escape <i>character</i> source { interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> }] * - Establish a connection to an IPv6 Stelnet server based on Suite B: ssh2 ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [-i <i>interface-type</i> <i>interface-number</i>] [prefer-compress zlib] [dscp <i>dscp-value</i> escape <i>character</i> source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 Stelnet servers.

Establishing a connection to an SFTP server based on Suite B

Task	Command	Remarks
Establish a connection to an SFTP server based on Suite B.	- Establish a connection to an IPv4 SFTP server based on Suite B: sftp server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [prefer-compress zlib] [dscp <i>dscp-value</i> source { interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> }] * - Establish a connection to an IPv6 SFTP server based on Suite B: sftp ipv6 server [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] suite-b [128-bit 192-bit] pki-domain <i>domain-name</i> [server-pki-domain <i>domain-name</i>] [-i <i>interface-type</i> <i>interface-number</i>] [prefer-compress zlib] [dscp <i>dscp-value</i> source { interface <i>interface-type</i> <i>interface-number</i> ipv6 <i>ipv6-address</i> }] *	Available in user view. The client cannot establish connections to both IPv4 and IPv6 SFTP servers.

Establishing a connection to an SCP server based on Suite B

Task	Command	Remarks
Establish a connection to an SCP server based on Suite B.	- Establish a connection to an IPv4 SCP server based on Suite B: <code>scp server [port-number] [vpn-instance vpn-instance-name] { put get } source-file-name [destination-file-name] suite-b [128-bit 192-bit] pki-domain domain-name [server-pki-domain domain-name] [prefer-compress zlib] [source { interface interface-type interface-number ip ip-address }] *</code> - Establish a connection to an IPv6 SCP server based on Suite B: <code>scp ipv6 server [port-number] [vpn-instance vpn-instance-name] [-i interface-type interface-number] { put get } source-file-name [destination-file-name] suite-b [128-bit 192-bit] pki-domain domain-name [server-pki-domain domain-name] [prefer-compress zlib] [source { interface interface-type interface-number ipv6 ipv6-address }] *</code>	Available in user view. The client cannot establish connections to both IPv4 and IPv6 SCP servers.

Specifying algorithms for SSH2

Perform this task to specify the following types of algorithms that the SSH2 client and server use for algorithm negotiation during the Stelnet, SFTP, or SCP session establishment:

- Key exchange algorithms.
- Public key algorithms.
- Encryption algorithms.
- MAC algorithms.

If you specify algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The client uses the specified algorithms to initiate the negotiation, and the server uses the matching algorithms to negotiate with the client.

If multiple algorithms of the same type are specified, the algorithm specified earlier has a higher priority during negotiation.

Specifying key exchange algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	<code>system-view</code>	N/A
2. Specify key exchange algorithms for SSH2.	- In non-FIPS mode: <code>ssh2 algorithm key-exchange { dh-group-exchange-sha1 dh-group1-sha1 dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } *</code> - In FIPS mode:	By default, SSH2 uses the key exchange algorithms <code>ecdh-sha2-nistp256</code> , <code>ecdh-sha2-nistp384</code> , <code>dh-group-exchange-sha1</code> , <code>dh-group14-sha1</code> , and <code>dh-group1-sha1</code> in descending order of priority for algorithm negotiation.

Step	Command	Remarks
	<pre>ssh2 algorithm key-exchange { dh-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 } *</pre>	

Specifying public key algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify public key algorithms for SSH2.	- In non-FIPS mode: <pre>ssh2 algorithm public-key { dsa ecdsa rsa x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } *</pre> - In FIPS mode: <pre>ssh2 algorithm public-key { ecdsa rsa x509v3-ecdsa-sha2-nistp384 x509v3-ecdsa-sha2-nistp256 } *</pre>	By default, SSH2 uses the public key algorithms x509v3-ecdsa-sha2-nistp256 , x509v3-ecdsa-sha2-nistp384 , ecdsa , rsa , and dsa in descending order of priority for algorithm negotiation.

Specifying encryption algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify encryption algorithms for SSH2.	- In non-FIPS mode: <pre>ssh2 algorithm cipher { 3des-cbc aes128-cbc aes256-cbc des-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } *</pre> - In FIPS mode: <pre>ssh2 algorithm cipher { aes128-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm } *</pre>	By default, SSH2 uses the encryption algorithms aes128-ctr , aes192-ctr , aes256-ctr , aes128-gcm , aes256-gcm , aes128-cbc , 3des-cbc , aes256-cbc , and des-cbc in descending order of priority for algorithm negotiation.

Specifying MAC algorithms for SSH2

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify MAC algorithms for SSH2.	- In non-FIPS mode: <pre>ssh2 algorithm mac { md5 md5-96 sha1 sha1-96 sha2-256 sha2-512 } *</pre> - In FIPS mode: <pre>ssh2 algorithm mac { sha1 sha1-96 sha2-256 sha2-512 } *</pre>	By default, SSH2 uses the MAC algorithms sha2-256 , sha2-512 , sha1 , md5 , sha1-96 , and md5-96 in descending order of priority for algorithm negotiation.

Command reference

New command: display ssh2 algorithm

Use **display ssh2 algorithm** to display algorithms used by SSH2 in the algorithm negotiation stage.

Syntax

display ssh2 algorithm

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display algorithms used by SSH2 in the algorithm negotiation stage.

```
<Sysname> display ssh2 algorithm
```

```
Key exchange algorithms : ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
```

```
Public key algorithms : x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384 ecdsa rsa
dsa
```

```
Encryption algorithms : aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm
aes128-cbc 3des-cbc aes256-cbc des-cbc
```

```
MAC algorithms : sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

Table 8 Command output

Field	Description
Key exchange algorithms	Key exchange algorithms in descending order of priority for algorithm negotiation.
Public key algorithms	Public key algorithms in descending order of priority for algorithm negotiation.
Encryption algorithms	Encryption algorithms in descending order of priority for algorithm negotiation.
MAC algorithms	MAC algorithms in descending order of priority for algorithm negotiation.

New command: ssh server pki-domain

Use **ssh server pki-domain** to specify a PKI domain for the SSH server.

Use **undo ssh server pki-domain** to delete the PKI domain of the SSH server.

Syntax

ssh server pki-domain *domain-name*

undo ssh server pki-domain

Default

No PKI domain is specified for an SSH server.

Views

System view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the name of a PKI domain, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 9](#).

Table 9 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Examples

Specify the PKI domain **serverpkidomain** for the SSH server.

```
<Sysname> system-view
```

```
[Sysname] ssh server pki-domain serverpkidomain
```

New command: scp ipv6 suite-b

Use **scp ipv6 suite-b** to establish a connection to an IPv6 SCP server based on Suite B algorithms and transfer files with the server.

Syntax

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] { put | get } source-file-name [ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i *interface-type interface-number*: Specifies an output interface by its type and number for SCP packets. Specify this option when the server uses a link-local address to provide the SCP service for the client. The specified output interface on the SCP client must have a link-local address.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file.

destination-file-name: Specifies the name of the target file. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see [Table 11](#).

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain domain-name: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 10](#).

Table 10 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain domain-name: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 10](#).

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

source: Specifies a source IPv6 address or source interface for IPv6 SCP packets. By default, the device automatically selects a source address for IPv6 SCP packets in compliance with RFC 3484. For successful SCP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv6 address of the loopback interface as the source IPv6 address.

interface interface-type interface-number: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IPv6 address of the IPv6 SCP packets.

ipv6 ipv6-address: Specifies a source IPv6 address.

Usage guidelines

Table 11 Suite B algorithms

Security level	Key exchange algorithm	Encryption algorithm and HMAC algorithm	Public key algorithm
128-bit	ecdh-sha2-nistp256	AEAD_AES_128_GCM	x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
192-bit	ecdh-sha2-nistp384	AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp384
Both	ecdh-sha2-nistp256	AEAD_AES_128_GCM	x509v3-ecdsa-sha2-nistp256

	ecdh-sha2-nistp384	AEAD_AES_256_GCM	x509v3-ecdsa-sha2-nistp384

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 192-bit Suite B algorithms to establish a connection to the SCP sever **2000::1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
```

New command: scp suite-b

Use **scp suite-b** to establish a connection to an SCP server based on Suite B algorithms and transfer files with the server.

Syntax

```
scp server [ port-number ] [ vpn-instance vpn-instance-name ] { put | get } source-file-name
[ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain
domain-name ] [ prefer-compress zlib ] [ source { interface interface-type interface-number | ip
ip-address } ] *
```

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

get: Downloads the file.

put: Uploads the file.

source-file-name: Specifies the name of the source file.

destination-file-name: Specifies the name of the target file. If you do not specify this argument, the target file uses the same file name as the source file.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see [Table 11](#).

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 12](#).

Table 12 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 12](#).

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

source: Specifies a source IP address or source interface for SCP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SCP packets. For successful SCP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv4 address of the loopback interface as the source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv4 address of this interface is the source IPv4 address of the SCP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 128-bit Suite B algorithms to establish a connection to the SCP sever **200.1.1.1** and download the file **abc.txt** from the server. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain  
server-pki-domain serverpkidomain
```

New command: sftp ipv6 suite-b

Use **sftp ipv6 suite-b** to establish a connection to an IPv6 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

sftp ipv6 *server* [*port-number*] [**vpn-instance** *vpn-instance-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**-i** *interface-type interface-number*]

[**prefer-compress** **zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i interface-type interface-number: Specifies an output interface by its type and number for IPv6 SFTP packets. Specify this option when the server uses a link-local address to provide the SFTP service for the client. The specified output interface on the SFTP client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see [Table 11](#).

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 13](#).

Table 13 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 13](#).

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for IPv6 SFTP packets. By default, the device automatically selects a source address for IPv6 SFTP packets in compliance with RFC 3484. For successful IPv6 SFTP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv6 address of the loopback interface as the source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SFTP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 192-bit Suite B algorithms to establish a connection to the SFTP sever **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

New command: sftp suite-b

Use **sftp suite-b** to establish a connection to an IPv4 SFTP server based on Suite B algorithms and enter SFTP client view.

Syntax

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b [ 128-bit | 192-bit ]
pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ dscp
dscp-value | source { interface interface-type interface-number | ip ip-address } ] *
```

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range of 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see [Table 11](#).

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 14](#).

Table 14 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 14](#).

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SFTP packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

source: Specifies a source IP address or source interface for the SFTP packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SFTP packets. For successful SFTP connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv4 address of the loopback interface as the source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SFTP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

Examples

Use the 128-bit Suite B algorithms to establish a connection to the SFTP sever **10.1.1.2**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
```

New command: ssh2 ipv6 suite-b

Use **ssh2 ipv6 suite-b** to establish a connection to an IPv6 Stelnet server based on Suite B algorithms.

Syntax

```
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b [ 128-bit | 192-bit ]
pki-domain domain-name [ server-pki-domain domain-name ] [ -i interface-type interface-number ]
```


[**prefer-compress** **zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type* *interface-number* | **ipv6** *ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv6 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

-i interface-type interface-number: Specifies an output interface by its type and number for IPv6 SSH packets. Specify this option when the server uses a link-local address to provide the Stelnet service for the client. The specified output interface on the Stelnet client must have a link-local address.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see [Table 11](#).

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 15](#).

Table 15 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 15](#).

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv6 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for IPv6 SSH packets. By default, the device automatically selects a source address for IPv6 SSH packets in compliance with RFC 3484. For successful IPv6 Stelnet connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv6 address of the loopback interface as the source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The IPv6 address of this interface is the source IP address of the IPv6 SSH packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. H3C recommends that you use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 192-bit Suite B algorithms to establish a connection to the Stelnet sever **2000::1**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain  
serverpkidomain
```

New command: ssh2 suite-b

Use **ssh2 suite-b** to establish a connection to an IPv4 Stelnet server based on Suite B algorithms.

Syntax

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b [ 128-bit | 192-bit ]  
pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ dscp  
dscp-value | escape character | source { interface interface-type interface-number | ip ip-address } ]  
*
```

Views

User view

Predefined user roles

network-admin

Parameters

server: Specifies a server by its IPv4 address or host name, a case-insensitive string of 1 to 253 characters.

port-number: Specifies the port number of the server, in the range 1 to 65535. The default is 22.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

suite-b: Specifies the Suite B algorithms. If neither the **128-bit** keyword nor the **192-bit** keyword is specified, all algorithms in Suite B are used. For more information about the Suite B algorithms, see [Table 11](#).

128-bit: Specifies the 128-bit Suite B security level.

192-bit: Specifies the 192-bit Suite B security level.

pki-domain *domain-name*: Specifies the PKI domain of the client's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 16](#).

Table 16 Invalid characters for a PKI domain name

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

server-pki-domain *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters, excluding the characters listed in [Table 16](#).

prefer-compress: Specifies the preferred compression algorithm for data compression between the server and the client. By default, compression is not supported.

zlib: Specifies the compression algorithm **zlib**.

dscp *dscp-value*: Specifies the DSCP value in the IPv4 SSH packets. The value range for the *dscp-value* argument is 0 to 63, and the default value is 48. The DSCP value determines the transmission priority of the packet.

escape *character*: Specifies a case-sensitive escape character. By default, the escape character is a tilde (~).

source: Specifies a source IP address or source interface for SSH packets. By default, the device uses the primary IPv4 address of the output interface in the routing entry as the source address of SSH packets. For successful Stelnet connections, use one of the following methods:

- Specify the loopback interface as the source interface.
- Specify the IPv4 address of the loopback interface as the source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number. The primary IPv4 address of this interface is the source IPv4 address of the SSH packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

If the client and the server have negotiated to use certificate authentication, the client must verify the server's certificate. For the client to correctly get the server's certificate, you must specify the server's PKI domain on the client by using the **server-pki-domain** *domain-name* option. The client uses the CA certificate stored in the specified PKI domain to verify the server's certificate and does not need to save the server's public key before authentication. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The combination of an escape character and a dot (.) works as an escape sequence. This escape sequence is typically used to quickly terminate an SSH connection when the server reboots or malfunctions.

For the escape sequence to take effect, you must enter it at the very beginning of a line. If you have entered other characters or performed operations in a line, enter the escape sequence in the next line. H3C recommends that you use the default escape character (~). Do not use any character in SSH usernames as the escape character.

Examples

Use the 128-bit Suite B algorithms to establish a connection to the SFTP sever **3.3.3.3**. Specify the client's PKI domain and the server's PKI domain as **clientpkidomain** and **serverpkidomain**, respectively.

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain  
serverpkidomain
```

New command: ssh2 algorithm cipher

Use **ssh2 algorithm cipher** to specify encryption algorithms for SSH2.

Use **undo ssh2 algorithm cipher** to restore the default.

Syntax

In non-FIPS mode:

```
ssh2 algorithm cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr  
| aes256-ctr | aes128-gcm | aes256-gcm } *
```

```
undo ssh2 algorithm cipher
```

In FIPS mode:

```
ssh2 algorithm cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr |  
aes128-gcm | aes256-gcm } *
```

```
undo ssh2 algorithm cipher
```

Default

SSH2 uses the encryption algorithms **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-gcm**, **aes256-gcm**, **aes128-cbc**, **3des-cbc**, **aes256-cbc**, and **des-cbc** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

3des-cbc: Specifies the encryption algorithm **3des-cbc**. Support for this keyword depends on the device model.

aes128-cbc: Specifies the encryption algorithm **aes128-cbc**.

aes256-cbc: Specifies the encryption algorithm **aes256-cbc**.

des-cbc: Specifies the encryption algorithm **des-cbc**.

aes128-ctr: Specifies the encryption algorithm **aes128-ctr**.

aes192-ctr: Specifies the encryption algorithm **aes192-ctr**.

aes256-ctr: Specifies the encryption algorithm **aes256-ctr**.

aes256-gcm: Specifies the encryption algorithm **aes256-gcm**.

aes128-gcm: Specifies the encryption algorithm **aes128-gcm**.

Usage guidelines

If you specify the encryption algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

Specify the algorithm **3des-cbc** as the encryption algorithm for SSH2.

```
<Sysname> system-view
```

```
[Sysname] ssh2 algorithm cipher 3des-cbc
```

New command: ssh2 algorithm key-exchange

Use **ssh2 algorithm key-exchange** to specify key exchange algorithms for SSH2.

Use **undo ssh2 algorithm key-exchange** to restore the default.

Syntax

In non-FIPS mode:

```
ssh2 algorithm key-exchange { dh-group-exchange-sha1 | dh-group1-sha1 |  
dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } *
```

```
undo ssh2 algorithm key-exchange
```

In FIPS mode:

```
ssh2 algorithm key-exchange { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 }  
*
```

```
undo ssh2 algorithm key-exchange
```

Default

SSH2 uses the key exchange algorithms **ecdh-sha2-nistp256**, **ecdh-sha2-nistp384**, **dh-group-exchange-sha1**, **dh-group14-sha1**, and **dh-group1-sha1** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dh-group-exchange-sha1: Specifies the key exchange algorithm **diffie-hellman-group-exchange-sha1**.

dh-group1-sha1: Specifies the key exchange algorithm **diffie-hellman-group1-sha1**.

dh-group14-sha1: Specifies the key exchange algorithm **diffie-hellman-group14-sha1**.

ecdh-sha2-nistp256: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.

ecdh-sha2-nistp384: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

Usage guidelines

If you specify the key exchange algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

```
# Specify the algorithm dh-group1-sha1 as the key exchange algorithm for SSH2.  
<Sysname> system-view  
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

New command: ssh2 algorithm mac

Use **ssh2 algorithm mac** to specify MAC algorithms for SSH2.

Use **undo ssh2 algorithm mac** to restore the default.

Syntax

In non-FIPS mode:

```
ssh2 algorithm mac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } *  
undo ssh2 algorithm mac
```

In FIPS mode:

```
ssh2 algorithm mac { sha1 | sha1-96 | sha2-256 | sha2-512 } *  
undo ssh2 algorithm mac
```

Default

SSH2 uses the MAC algorithms **sha2-256**, **sha2-512**, **sha1**, **md5**, **sha1-96**, and **md5-96** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies the HMAC algorithm **hmac-md5**.

md5-96: Specifies the HMAC algorithm **hmac-md5-96**.

sha1: Specifies the HMAC algorithm **hmac-sha1**.

sha1-96: Specifies the HMAC algorithm **hmac-sha1-96**.

sha2-256: Specifies the HMAC algorithm **hmac-sha2-256**.

sha2-512: Specifies the HMAC algorithm **hmac-sha2-512**.

Usage guidelines

If you specify the MAC algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

```
# Specify the algorithm md5 as the MAC algorithm for SSH2.  
<Sysname> system-view  
[Sysname] ssh2 algorithm mac md5
```

New command: ssh2 algorithm public-key

Use **ssh2 algorithm public-key** to specify public key algorithms for SSH2.

Use **undo ssh2 algorithm public-key** to restore the default.

Syntax

In non-FIPS mode:

```
ssh2 algorithm public-key { dsa | ecdsa | rsa | x509v3-ecdsa-sha2-nistp384 |  
x509v3-ecdsa-sha2-nistp256 } *
```

```
undo ssh2 algorithm public-key
```

In FIPS mode:

```
ssh2 algorithm public-key { ecdsa | rsa | x509v3-ecdsa-sha2-nistp384 |  
x509v3-ecdsa-sha2-nistp256 } *
```

```
undo ssh2 algorithm public-key
```

Default

SSH2 uses the public key algorithms **x509v3-ecdsa-sha2-nistp256**, **x509v3-ecdsa-sha2-nistp384**, **ecdsa**, **rsa**, and **dsa** in descending order of priority for algorithm negotiation.

Views

System view

Predefined user roles

network-admin

Parameters

dsa: Specifies the public key algorithm **dsa**.

ecdsa: Specifies the public key algorithm **ecdsa**.

rsa: Specifies the public key algorithm **rsa**.

x509v3-ecdsa-sha2-nistp256: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.

x509v3-ecdsa-sha2-nistp384: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.

Usage guidelines

If you specify the public key algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The algorithm specified earlier has a higher priority during negotiation.

Examples

```
# Specify the algorithm dsa as the public key algorithm for SSH2.
```

```
<Sysname> system-view
```

```
[Sysname] ssh2 algorithm public-key dsa
```

Modified command: display ssh server

Syntax

```
display ssh server { session | status }
```

Views

Any view

Change description

In the command output, the **SSH Server PKI domain name** field was added to represent the PKI domain of the SSH server.

Modified command: ssh user

Old syntax

In non-FIPS mode:

```
ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type
{ password | { any | password-publickey | publickey } assign { pki-domain domain-name |
publickey keyname } }
```

```
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type
{ password | password-publickey assign { pki-domain domain-name | publickey keyname } }
```

```
undo ssh user username
```

New syntax

In non-FIPS mode:

```
ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type
{ password | { any | password-publickey | publickey } [ assign { pki-domain domain-name |
publickey keyname } ] }
```

```
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type
{ password | password-publickey [ assign { pki-domain domain-name | publickey keyname } ] }
```

```
undo ssh user username
```

Views

System view

Change description

Before modification: The options **assign** { pki-domain domain-name | publickey keyname } are required for verifying the client.

After modification: The options **assign** { pki-domain domain-name | publickey keyname } are optional for verifying the client.

Modified command: scp

Old syntax

In non-FIPS mode:

```
scp server [ port-number ] [ vpn-instance vpn-instance-name ] { put | get } source-file-name
[ destination-file-name ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher
{ 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex
{ dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 |
des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] * [ publickey keyname | source
{ interface interface-type interface-number | ip ip-address } ] *
```

In FIPS mode:

```
scp server [ port-number ] [ vpn-instance vpn-instance-name ] { put | get } source-file-name
[ destination-file-name ] [ identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 |
aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher
```

```
{ aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] * [ publickey keyname | source
{ interface interface-type interface-number | ip ip-address } ] *
```

New syntax

In non-FIPS mode:

```
scp server [ port-number ] [ vpn-instance vpn-instance-name ] { put | get } source-file-name
[ destination-file-name ] [ identity-key { dsa | ecdsa | rsa | { x509v3-ecdsa-sha2-nistp384 |
x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } | prefer-compress zlib |
prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 |
dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |
aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm |
aes256-gcm } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] *
[ { public-key keyname | server-pki-domain domain-name } | source { interface interface-type
interface-number | ip ip-address } ] *
```

In FIPS mode:

```
scp server [ port-number ] [ vpn-instance vpn-instance-name ] { put | get } source-file-name
[ destination-file-name ] [ identity-key { ecdsa | rsa | { x509v3-ecdsa-sha2-nistp384 |
x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } | prefer-compress zlib |
prefer-ctos-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr |
aes128-gcm | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } |
prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher
{ aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } |
prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ { public-key keyname |
server-pki-domain domain-name } | source { interface interface-type interface-number | ip
ip-address } ] *
```

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
 - pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
 - server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
 - **ecdsa**: Specifies the public key algorithm **ecdsa**.
 - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
 - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
 - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
 - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
 - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
 - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
 - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
 - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
 - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
 - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
 - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
 - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
 - The **dh-group1** keyword was changed to **dh-group1-sha1**.
 - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
 - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.

- After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.

Modified command: scp ipv6

Old syntax

In non-FIPS mode:

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type
interface-number ] { put | get } source-file-name [ destination-file-name ] [ identity-key { dsa | rsa }
| prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac
{ md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } |
prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 |
sha1-96 } ] * [ publickey keyname | source { interface interface-type interface-number | ipv6
ipv6-address } ] *
```

In FIPS mode:

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type
interface-number ] { put | get } source-file-name [ destination-file-name ] [ identity-key rsa |
prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 |
sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac
{ sha1 | sha1-96 } ] * [ publickey keyname | source { interface interface-type interface-number |
ipv6 ipv6-address } ] *
```

New syntax

In non-FIPS mode:

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type
interface-number ] { put | get } source-file-name [ destination-file-name ] [ identity-key { dsa | ecdsa
| rsa | { x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name }
| prefer-compress zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc |
aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { md5 |
md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 |
dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ { public-key keyname | server-pki-domain domain-name } | source
{ interface interface-type interface-number | ipv6 ipv6-address } ] *
```

In FIPS mode:

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type
interface-number ] { put | get } source-file-name [ destination-file-name ] [ identity-key { ecdsa | rsa
| { x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } |
prefer-compress zlib | prefer-ctos-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 |
sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr |
aes128-gcm | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] *
[ { public-key keyname | server-pki-domain domain-name } | source { interface interface-type
interface-number | ipv6 ipv6-address } ] *
```

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
 - pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
 - server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
 - ecdsa**: Specifies the public key algorithm **ecdsa**.
 - x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
 - x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
 - aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
 - aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
 - aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
 - aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
 - aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
 - sha2-256**: Specifies the HMAC algorithm **sha2-256**.
 - sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
 - ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
 - ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.

- The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
 - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
 - The **dh-group1** keyword was changed to **dh-group1-sha1**.
 - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
 - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
 - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.

Modified command: sftp

Old syntax

In non-FIPS mode:

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] * [ dscp dscp-value | publickey keyname | source { interface interface-type interface-number | ip ip-address } ] *
```

In FIPS mode:

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] * [ publickey keyname | source { interface interface-type interface-number | ip ip-address } ] *
```

New syntax

In non-FIPS mode:

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | ecdsa | rsa |  
{ x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } |  
prefer-compress zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc |  
aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { md5 |  
md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 |  
dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |  
prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr |  
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |  
sha2-256 | sha2-512 } ] * [ dscp dscp-value | { public-key keyname | server-pki-domain  
domain-name } | source { interface interface-type interface-number | ip ip-address } ] *
```

In FIPS mode:

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { ecdsa | rsa |  
{ x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } |  
prefer-compress zlib | prefer-ctos-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr |  
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 |  
sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |  
prefer-stoc-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr |  
aes128-gcm | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] *  
[ { public-key keyname | server-pki-domain domain-name } | source { interface interface-type  
interface-number | ip ip-address } ] *
```

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
 - pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
 - server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
 - ecdsa**: Specifies the public key algorithm **ecdsa**.

- **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
- **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
 - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
 - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
 - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
 - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
 - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
 - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
 - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
 - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
 - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
 - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
 - The **dh-group1** keyword was changed to **dh-group1-sha1**.
 - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
 - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
 - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:

- Before modification: The default is **aes128**.
- After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.

Modified command: sftp ipv6

Old syntax

In non-FIPS mode:

```
sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] * [ dscp dscp-value | publickey keyname | source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

In FIPS mode:

```
sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] * [ publickey keyname | source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

New syntax

In non-FIPS mode:

```
sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key { dsa | ecdsa | rsa | { x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } } | pki-domain domain-name } | prefer-compress zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ dscp dscp-value | { public-key keyname | server-pki-domain domain-name } | source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

In FIPS mode:

```
sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key { ecdsa | rsa | { x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } } | pki-domain domain-name } | prefer-compress zlib | prefer-ctos-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ { public-key keyname | server-pki-domain domain-name } | source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
 - pki-domain** *domain-name*: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
 - server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.
- The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
 - ecdsa**: Specifies the public key algorithm **ecdsa**.
 - x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
 - x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
 - aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
 - aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
 - aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
 - aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
 - aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
 - sha2-256**: Specifies the HMAC algorithm **sha2-256**.
 - sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
 - ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
 - ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
 - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.

- The **dh-group1** keyword was changed to **dh-group1-sha1**.
 - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
 - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
 - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.

Modified command: ssh2

Old syntax

In non-FIPS mode:

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | rsa } |
prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac
{ md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } |
prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 |
sha1-96 } ] * [ dscp dscp-value | escape character | publickey keyname | source { interface
interface-type interface-number | ip ip-address } ] *
```

In FIPS mode:

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key rsa |
prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 |
sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac
{ sha1 | sha1-96 } ] * [ escape character | publickey keyname | source { interface interface-type
interface-number | ip ip-address } ] *
```

New syntax

In non-FIPS mode:

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | ecdsa | rsa |
{ x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } |
```

```
prefer-compress zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc |
aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { md5 |
md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 |
dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ dscp dscp-value | escape character | { public-key keyname |
server-pki-domain domain-name } | source { interface interface-type interface-number | ip
ip-address } ] *
```

In FIPS mode:

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { ecdsa | rsa |
{ x509v3-ecdsa-sha2-nistp384 | x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } |
prefer-compress zlib | prefer-ctos-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr |
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 |
sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr |
aes128-gcm | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] *
[ escape character | { public-key keyname | server-pki-domain domain-name } | source
{ interface interface-type interface-number | ip ip-address } ] *
```

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
 - pki-domain domain-name**: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.
 - server-pki-domain domain-name**: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
 - ecdsa**: Specifies the public key algorithm **ecdsa**.
 - x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
 - x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:

- **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
- **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
- **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
- **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
- **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
 - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
 - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
 - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
 - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
 - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
 - The **dh-group1** keyword was changed to **dh-group1-sha1**.
 - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
 - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
 - After modification: The default is **ecdh-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.

Modified command: ssh2 ipv6

Old syntax

In non-FIPS mode:

```
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type  
interface-number ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des |  
aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex  
{ dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 |  
des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } ] * [ dscp dscp-value | escape  
character | publickey keyname | source { interface interface-type interface-number | ipv6  
ipv6-address } ] *
```

In FIPS mode:

```
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type  
interface-number ] [ identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 |  
aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher  
{ aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } ] * [ escape character | publickey  
keyname | source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

New syntax

In non-FIPS mode:

```
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type  
interface-number ] [ identity-key { dsa | ecdsa | rsa | { x509v3-ecdsa-sha2-nistp384 |  
x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } | prefer-compress zlib |  
prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr |  
aes256-ctr | aes128-gcm | aes256-gcm } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 |  
sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 |  
dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |  
aes128-cbc | aes256-cbc | des-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm |  
aes256-gcm } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] *  
[ dscp dscp-value | escape character | { public-key keyname | server-pki-domain domain-name }  
| source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

In FIPS mode:

```
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type  
interface-number ] [ identity-key { ecdsa | rsa | { x509v3-ecdsa-sha2-nistp384 |  
x509v3-ecdsa-sha2-nistp256 } pki-domain domain-name } | prefer-compress zlib |  
prefer-ctos-cipher { aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr |  
aes128-gcm | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } |  
prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher  
{ aes128-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm | aes256-gcm } |  
prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ escape character | { public-key  
keyname | server-pki-domain domain-name } | source { interface interface-type interface-number  
| ipv6 ipv6-address } ] *
```

Views

User view

Change description

The following keywords were added:

- Keywords for specifying PKI domains used in certificate verification:
 - **pki-domain domain-name**: Specifies the PKI domain of the client's certificate. When the public key algorithm is x509v3 (**x509v3-ecdsa-sha2-nistp256** or **x509v3-ecdsa-sha2-nistp384**), you must specify this option for the client to get the correct local certificate.

- **server-pki-domain** *domain-name*: Specifies the PKI domain for verifying the server's certificate. The *domain-name* argument represents the PKI domain name, a case-insensitive string of 1 to 31 characters. If you do not specify the server's PKI domain, the client uses the PKI domain of its own certificate to verify the server's certificate.

The PKI domain name cannot contain characters in the following table:

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

- Keywords for specifying the publickey algorithms used in publickey authentication:
 - **ecdsa**: Specifies the public key algorithm **ecdsa**.
 - **x509v3-ecdsa-sha2-nistp256**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp256**.
 - **x509v3-ecdsa-sha2-nistp384**: Specifies the public key algorithm **x509v3-ecdsa-sha2-nistp384**.
- Keywords for specifying the preferred client-to-server encryption algorithms:
 - **aes128-ctr**: Specifies the encryption algorithm **aes128-ctr**.
 - **aes192-ctr**: Specifies the encryption algorithm **aes192-ctr**.
 - **aes256-ctr**: Specifies the encryption algorithm **aes256-ctr**.
 - **aes256-gcm**: Specifies the encryption algorithm **aes256-gcm**.
 - **aes128-gcm**: Specifies the encryption algorithm **aes128-gcm**.
- Keywords for specifying the preferred client-to-server HMAC algorithms:
 - **sha2-256**: Specifies the HMAC algorithm **sha2-256**.
 - **sha2-512**: Specifies the HMAC algorithm **sha2-512**.
- Keywords for specifying the preferred key exchange algorithms:
 - **ecdh-sha2-nistp256**: Specifies the key exchange algorithm **ecdh-sha2-nistp256**.
 - **ecdh-sha2-nistp384**: Specifies the key exchange algorithm **ecdh-sha2-nistp384**.

The following keywords were modified:

- Keywords for the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.
 - The **aes128** keyword was changed to **aes128-cbc**.
 - The **aes256** keyword was changed to **aes256-cbc**.
 - The **des** keyword was changed to **des-cbc**.
- Keywords for the preferred key exchange algorithm **prefer-kex**:
 - The **dh-group-exchange** keyword was changed to **dh-group-exchange-sha1**.
 - The **dh-group1** keyword was changed to **dh-group1-sha1**.
 - The **dh-group14** keyword was changed to **dh-group14-sha1**.
- Keywords for the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - The **3des** keyword was changed to **3des-cbc**.

- The **aes128** keyword was changed to **aes128-cbc**.
- The **aes256** keyword was changed to **aes256-cbc**.
- The **des** keyword was changed to **des-cbc**.

The default settings for the following algorithms were changed:

- For the preferred client-to-server encryption algorithm **prefer-ctos-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred client-to-server HMAC algorithm **prefer-ctos-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.
- For the preferred key exchange algorithm **prefer-kex**:
 - Before modification: The default is **dh-group-exchange** in non-FIPS mode and is **dh-group14** in FIPS mode.
 - After modification: The default is **ecdhe-sha2-nistp256** in both non-FIPS mode and FIPS mode.
- For the preferred server-to-client encryption algorithm **prefer-stoc-cipher**:
 - Before modification: The default is **aes128**.
 - After modification: The default is **aes128-ctr**.
- For the preferred server-to-client HMAC algorithm **prefer-stoc-hmac**:
 - Before modification: The default is **sha1**.
 - After modification: The default is **sha2-256**.

New command: fips kdf ssh

Use **fips kdf ssh** to generate a validation file in SSH Key Derivation Function (KDF) test.

Syntax

fips kdf ssh import *single-request-file* **export** *validation-file*

Views

Probe view

Predefined user roles

network-admin

Parameters

import *single-request-file*: Specifies the name of the single request file generated by CAVS.

export *validation-file*: Specifies a name for the validation file to be generated.

Usage guidelines

SSH gets parameters from the single request file and sends them to the key derivation module. After the key derivation module returns the calculation result, SSH stores the calculation result in the validation file.

Examples

Specify **ssh.req** and **ssh.txt** as the single request file and the validation file, respectively.

```
<Sysname> system-view
```

```
[Sysname] probe
```

```
[Sysname-probe] fips ssh kdf import ssh.req export ssh.txt
```

New feature: EVPN

Configuring EVPN

For information about EVPN configuration, see *H3C MSR Router Series Comware 7 EVPN Configuration Guide*.

Command reference

For information about EVPN commands, see *H3C MSR Router Series Comware 7 EVPN Command Reference*.

New feature: SM2 key pair creation

Creating an SM2 key pair

You can create an SM2 key pair in non-FIPS mode.

To create an SM2 key pair:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Creating an SM2 key pair.	public-key local create sm2 [name <i>key-name</i>] [on <i>device-name</i>]	By default, no SM2 key pairs exist. Support for this command depends on the device model.

Command reference

New command: public-key local create sm2

Syntax

public-key local create sm2 [**name** *key-name*] [**on** *device-name*]

Default

No SM2 key pairs exist.

Views

System view

Predefined user roles

network-admin

Parameters

name *key-name*: Assigns a name to the SM2 key pair. The *key-name* argument is a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, and hyphens (-). If you do not assign a name to the key pair, the key pair takes the default name (**sm2key**).

on device-name: Specifies the crypto device used to generate the SM2 key pair. The *device-name* argument specifies the device name, a case-sensitive string of 1 to 31 characters. If you do not specify a crypto device, the SM2 key pair will be created by a software algorithm. You can view the names of available crypto devices by entering a question mark (?) after the **on** keyword.

Usage guidelines

Support for this command depends on the device model.

This command creates a 256-bit SM2 host key pair.

If you do not assign the SM2 key pair a name, the system assigns the default name to the key pair and marks the key pair as **default**. You can also assign the default name to another SM2 key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

The key pairs are automatically saved and can survive system reboots.

Examples

```
# Create a local SM2 key pair named sm2.
<Sysname> system-view
[Sysname] public-key local create sm2 name sm2
Generating Keys...
Create the key pair successfully.
```

New feature: Built-in AC

Configuring the built-in AC

For more information, see *H3C MSR Router Series Comware 7 WLAN AC Configuration Guide*.

Command reference

For more information, see *H3C MSR Router Series Comware 7 WLAN AC Command Reference*.

Release 0605P20

This release has the following changes:

[Modified feature: Authentication mode for accessing a 4G network](#)

Modified feature: Authentication mode for accessing a 4G network

Feature change description

In this release, the length of the username for authentication changed from 1 to 32 characters to 1 to 80 characters.

Command changes

Modified command: authentication-mode

Syntax

authentication-mode { **pap** | **chap** | **pap-chap** } **user** *user-name* **password** { **cipher** | **simple** } *string*

undo authentication-mode

Views

4G modem profile view

Change description

Before modification: The value range for the *user-name* argument is 1 to 32 characters.

After modification: The value range for the *user-name* argument is 1 to 80 characters.

Release 0605P13

This release has the following changes:

New feature: Associating Track with a tracked list

New feature: Associating Track with EAA

Modified feature: Support for ACLs in SNMP commands

Modified feature: NAT for the multicast source address in PIM join and prune messages

Modified feature: Setting the maximum number of concurrent FTP users

Modified feature: Portal authentication

New feature: Associating Track with a tracked list

Associating Track with a tracked list

For information about this feature, see *H3C MSR Router Series Comware 7 High Availability Configuration Guide*.

Command reference

The following commands were newly added:

- **delay**
- **object**
- **threshold percentage**
- **threshold weight**
- **track list boolean**

- **track list threshold percentage**
- **track list threshold weight**

For more information about these commands, see *H3C MSR Router Series Comware 7 High Availability Command Reference*.

New feature: Associating Track with EAA

Associating Track with EAA

About Track association with EAA

You can configure EAA track event monitor policies to monitor the positive-to-negative or negative-to-positive state changes of track entries.

- If you specify only one track entry for a policy, EAA triggers the policy when it detects the specified state change on the track entry.
- If you specify multiple track entries for a policy, EAA triggers the policy when it detects the specified state change on the last monitored track entry. For example, if you configure a policy to monitor the positive-to-negative state change of multiple track entries, EAA triggers the policy when the last positive track entry monitored by the policy is changed to the Negative state.

You can set a suppression time for a track event monitor policy. The timer starts when the policy is triggered. The system does not process messages that report the monitored track event until the timer times out.

Procedure

To associate Track with EAA:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a CLI-defined monitor policy and enter its view, or enter the view of an existing CLI-defined monitor policy.	rtm cli-policy <i>policy-name</i>	By default, no CLI-defined monitor policies exist.
3. Configure a track event.	event track <i>track-entry-number-list</i> state { negative positive } [suppress-time <i>suppress-time</i>]	By default, a monitor policy does not contain any track event.

Command reference

event track

Use **event track** to configure a track event for a CLI-defined monitor policy.

Use **undo event** to delete the event in a CLI-defined monitor policy.

Syntax

event track *track-list* **state** { **negative** | **positive** } [**suppress-time** *suppress-time*]

undo event

Default

A CLI-defined policy does not contain a track event.

Views

CLI-defined policy view

Predefined user roles

network-admin

Parameters

track-list: Specifies a space-separated list of up to 16 track items. Each item specifies a track entry number or a range of track entry numbers in the form of *track-entry-number* **to** *track-entry-number*. The value range for the *track-entry-number* argument is 1 to 1024.

state { negative | positive }: Monitors state changes of the track entries.

- **negative**: Triggers the policy when the state of the track entries changes from Positive to Negative.
- **positive**: Triggers the policy when the state of the track entries changes from Negative to Positive.

suppress-time *suppress-time*: Sets a suppress time in the range of 1 to 4294967295, in seconds. The default value is 0.

Usage guidelines

Use track event monitor policies to monitor state changes of track entries. If you specify one track entry for a policy, EAA triggers the policy when the state of the track entry changes from Positive to Negative or from Negative to Positive. If you specify multiple track entries for a policy, EAA triggers the policy only when the state of all the track entries changes from Positive (Negative) to Negative (Positive).

If you set a suppress time for a track event monitor policy, the timer starts when the policy is triggered. The system does not process the messages that report the track entry state change Positive (Negative) to Negative (Positive) until the timer times out.

For example, to automatically disconnect the sessions between the local device and its down link BGP peers when the sessions between the local device and its uplink BGP peers are disconnected, you can configure a track event monitor policy as follows:

- Configure a track event for the policy and specify track entries to monitor the links between the local device and its uplink BGP peers.
- Add CLI action **peer ignore** to the policy to disable BGP session establishment between the local device and its downlink BGP peers.

You can configure only one event entry for a monitor policy. If the monitor policy already contains an event entry, the new event entry replaces the old event entry.

Examples

Create CLI-defined monitor policy **test**. Configure a track event for the policy that occurs when the state of track entry 1 to track entry 8 changes from Positive to Negative. Set the suppress time to 180 seconds for the policy.

```
<Sysname>system-view
[Sysname] rtm cli-policy test
[Sysname-rtm-test] event track 1 to 8 state negative suppress-time 180
```

Modified feature: Support for ACLs in SNMP commands

Feature change description

In this release, you can specify an advanced ACL when you create or delete an SNMP group, community, or user.

Command changes

Modified command: snmp-agent community

Syntax

In VACM mode:

```
snmp-agent community { read | write } [ simple | cipher ] community-name [ mib-view view-name ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent community [ cipher ] community-name
```

In RBAC mode:

```
snmp-agent community [ simple | cipher ] community-name user-role role-name [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent community [ cipher ] community-name
```

Views

System view

Change description

Before modification, you can only specify a basic ACL by its number.

- *ipv4-acl-number*: Specifies a basic IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic IPv6 ACL by its number.

After modification, you can specify a basic or advanced ACL by its number.

- *ipv4-acl-number*: Specifies a basic or advanced IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic or advanced IPv6 ACL by its number.

Modified command: snmp-agent group

Syntax

SNMPv1 and SNMP v2c:

```
snmp-agent group { v1 | v2c } group-name [ read-view view-name ] [ write-view view-name ] [ notify-view view-name ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent group { v1 | v2c } group-name
```

SNMPv3 (in non-FIPS mode):

```
snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view ]
[ write-view write-view ] [ notify-view notify-view ] [ acl { ipv4-acl-number | name ipv4-acl-name } |
acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent group v3 group-name [ authentication | privacy ]
```

SNMPv3 (in FIPS mode):

```
snmp-agent group v3 group-name { authentication | privacy } [ read-view read-view ]
[ write-view write-view ] [ notify-view notify-view ] [ acl { ipv4-acl-number | name ipv4-acl-name } |
acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent group v3 group-name { authentication | privacy }
```

Views

System view

Change description

Before modification, you can only specify a basic ACL by its number.

- *ipv4-acl-number*: Specifies a basic IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic IPv6 ACL by its number.

After modification, you can specify a basic or advanced ACL by its number.

- *ipv4-acl-number*: Specifies a basic or advanced IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic or advanced IPv6 ACL by its number.

Modified command: snmp-agent usm-user

Syntax

```
snmp-agent usm-user { v1 | v2c } user-name group-name [ acl { ipv4-acl-number | name
ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent usm-user { v1 | v2c } user-name
```

Views

System view

Change description

Before modification, you can only specify a basic ACL by its number.

- *ipv4-acl-number*: Specifies a basic IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic IPv6 ACL by its number.

After modification, you can specify a basic or advanced ACL by its number.

- *ipv4-acl-number*: Specifies a basic or advanced IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic or advanced IPv6 ACL by its number.

Modified command: snmp-agent usm-user v3

Syntax

In non-FIPS mode (in VACM mode):

```
snmp-agent usm-user v3 user-name group-name [ remote { ipv4-address | ipv6 ipv6-address }
[ vpn-instance vpn-instance-name ] ] [ { cipher | simple } authentication-mode { md5 | sha }
auth-password [ privacy-mode { 3des | aes128 | aes192 | aes256 | des56 } priv-password ] ] [ acl
{ ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent usm-user v3 user-name { local | engineid engineid-string | remote
{ ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] }
```

In non-FIPS mode (in RBAC mode):

```
snmp-agent usm-user v3 user-name user-role role-name [ remote { ipv4-address | ipv6
ipv6-address } [ vpn-instance vpn-instance-name ] ] [ { cipher | simple } authentication-mode
{ md5 | sha } auth-password [ privacy-mode { 3des | aes128 | aes192 | aes256 | des56 }
priv-password ] ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name
ipv6-acl-name } ] *
```

```
undo snmp-agent usm-user v3 user-name { local | engineid engineid-string | remote
{ ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] }
```

In FIPS mode (in VACM mode):

```
snmp-agent usm-user v3 user-name group-name [ remote { ipv4-address | ipv6 ipv6-address }
[ vpn-instance vpn-instance-name ] ] { cipher | simple } authentication-mode sha auth-password
[ privacy-mode { aes128 | aes192 | aes256 } priv-password ] [ acl { ipv4-acl-number | name
ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent usm-user v3 user-name { local | engineid engineid-string | remote
{ ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] }
```

In FIPS mode (in RBAC mode):

```
snmp-agent usm-user v3 user-name user-role role-name [ remote { ipv4-address | ipv6
ipv6-address } [ vpn-instance vpn-instance-name ] ] [ { cipher | simple } authentication-mode
sha auth-password [ privacy-mode { aes128 | aes192 | aes256 } priv-password ] ] [ acl
{ ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
```

```
undo snmp-agent usm-user v3 user-name { local | engineid engineid-string | remote
{ ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] }
```

Views

System view

Change description

Before modification, you can only specify a basic ACL by its number.

- *ipv4-acl-number*: Specifies a basic IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic IPv6 ACL by its number.

After modification, you can specify a basic or advanced ACL by its number.

- *ipv4-acl-number*: Specifies a basic or advanced IPv4 ACL by its number.
- *ipv6-acl-number*: Specifies a basic or advanced IPv6 ACL by its number.

Modified feature: NAT for the multicast source address in PIM join and prune messages

Feature change description

In this release, you can configure NAT on the device to translate the multicast source address (a private address) in PIM join and prune messages to a private address. This feature is applicable to the scenario where PIM-SSM runs on the IPv4 network, multicast receivers reside on the public network, and the multicast source resides on a private network.

Modified feature: Setting the maximum number of concurrent FTP users

Feature change description

For the LA3616 wireless gateway, the value range for the maximum number of concurrent FTP users was changed at the CLI and NETCONF. Before modification, the value range is 1 to 32. After modification, the value range is 1 to 64.

Command changes

Modified command: `aaa session-limit ftp`

Syntax

`aaa session-limit ftp` *max-sessions*

`undo aaa session-limit ftp`

Views

System view

Change description

Before modification: The value range for the *max-sessions* argument is 1 to 32.

After modification: The value range for the *max-sessions* argument is 1 to 64.

Modified feature: Portal authentication

Feature change description

Before modification, an MSR router cannot redirect the HTTPS requests of unauthenticated users to the portal Web server. No portal authentication page is pushed to unauthenticated users if the users access the network by using the HTTPS protocol.

After modification, an MSR router can redirect the HTTPS requests of unauthenticated users to the portal Web server. The portal Web server will push the portal authentication page to unauthenticated users if the users access the network by using the HTTPS protocol.

Command changes

None.

Release 0415

None

Release 0413

This release has the following changes:

New feature: IP forwarding last hop holding

Modified feature: Temporary user role authorization

New feature: IP forwarding last hop holding

Configuring last hop holding

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 3 Ethernet interface view or subinterface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Enable last hop holding.	ip last-hop hold	By default, last hop holding is disabled.

Command reference

ip last-hop hold

Use **ip last-hop hold** to enable last hop holding.

Use **undo ip last-hop hold** to disable last hop holding.

Syntax

ip last-hop hold

undo ip last-hop hold

Default

Last hop holding is disabled.

Views

Layer 3 Ethernet interface view

Layer 3 Ethernet subinterface view

Predefined user roles

network-admin

Usage guidelines

Last hop holding implements symmetric routing. It tracks the last hop MAC address for the first outgoing IP packet of a connection, and it sends the return packets to the hop that transmits the request.

Last hop holding is based on fast forwarding entries. If the MAC address of a last hop changes, this feature can function correctly only after the fast forwarding entry is updated for the MAC address.

Examples

```
# Enable the last hop holding feature.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip last-hop hold
```

Modified feature: Temporary user role authorization

Feature change description

The security-audit user role was unavailable for temporary user role authorization.

Command changes

Modified command: super password

Syntax

In non-FIPS mode:

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

In FIPS mode:

super password [**role** *role-name*]

undo super password [**role** *role-name*]

Views

System view

Change description

The *role-name* argument cannot be security-audit. You can specify any existing user role in the system except security-audit and guest-manager for this argument.

Release 0411

None.

Release 0410

This release has the following changes:

New feature: [Support of multicast for ADVPN](#)

New feature: [Application layer state filtering](#)

New feature: [SIP keepalive](#)

New feature: [Multicast fast forwarding](#)

New feature: SSL support for POS terminal access

New feature: Attack defense policy application to a security zone

New feature: AAA support for IKE extended authentication

New feature: Percentage-based CAR

New feature: Logging OSPF router ID conflict events

New feature: AFT

New feature: Configuring enhanced CC authentication in FIPS mode

New feature: Support of AAA for NETCONF

New feature: Mobile IP tunnel interface settings

New feature: LISP

New feature: LISP tunnel entries and dynamic mobility

New feature: Support of IPv6 multicast routing for VPN instances

New feature: IPv4/IPv6 PIM NSR

New feature: IGMP/MLD NSR

New feature: IPv4/IPv6 PIM passive mode

New feature: LISP virtual machine multi-hop mobility and DDT

New feature: LISP NSR

New feature: PPPoE client support for IPv6

New feature: Frame-Relay-related functions

New feature: DPI engine and content filtering

New feature: IPS

New feature: NBAR

New feature: URL filtering

New feature: Local portal Web server

New feature: Support of portal for NETCONF

New feature: Newly-added MIB objects

New feature: Performing a loopback test

New feature: IPS, ACG, and SSL VPN licenses

New feature: Support of NQA for NETCONF

New feature: Configuring CWMP to support VPN

New feature: Transceiver module source alarm

New feature: VLAN interface performance optimization

New feature: POSA

New feature: Specifying a backup processing slot for an interface

New feature: Configuring the ISDN leased line

New feature: NAT support for multicast source address in PIM join/prune packets

New feature: GDOI GM group anti-replay window

New feature: SIP compatibility

New feature: Voice VLAN

New feature: L2TP-based EAD

New feature: Configuring device poweroff alarming

New feature: BFD for an aggregation group

New feature: 4G modem IMSI/SN binding authentication

New feature: Media Stream Control (MSC) logging

New feature: IMSI/SN binding authentication

New feature: Specifying a band for a 4G modem

New feature: Using tunnel interfaces as OpenFlow ports

New feature: NETCONF support for ACL filtering

New feature: WAAS

New feature: Support for the MKI field in SRTP or SRTCP packets

New feature: SIP domain name

New feature: E&M logging

New feature: Setting the RTC version

New feature: Setting the maximum size of advertisement files

New feature: Support of IRF for NETCONF

New feature: Support of VCF for NETCONF

New feature: Support of SNMP for NETCONF

New feature: Support of file system for NETCONF

New feature: Support of PoE for NETCONF

New feature: Support of RMON for NETCONF

New feature: Support of policy-based routing for NETCONF

New feature: Support of BGP for NETCONF

New feature: Support of OSPF for NETCONF

New feature: Support of ping for NETCONF

New feature: Support of traceroute for NETCONF

New feature: Support of L2VPN for NETCONF

New feature: SIP support for VRF

New feature: IKEv2

New feature: Specifying an IKEv2 profile for an IPsec policy

New feature: Bidirectional BFD control detection for RIP

New feature: OSPF router ID autoconfiguration

New feature: Layer 2 Ethernet link aggregation

New feature: Setting the cable impedance for WAN interfaces

New feature: Associating a static route with a track entry

New feature: VLAN tag processing rule for incoming traffic

New feature: IP-based portal-free rule

New feature: Portal redirect packet statistics

New feature: GDVPN

New feature: OpenFlow instance

New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set

New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy

New feature: SIP session refresh

Modified feature: License restrictions for POS terminal access

Modified feature: Displaying and maintaining Frame Relay

Modified feature: Displaying track entry information

Modified feature: User profile

Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes

Modified feature: PKI certificate auto-renewal

Modified feature: Configuring the PKI entity DN

Modified feature: ADVPN

Modified feature: Telnet redirect

Modified feature: DHCP snooping performance optimization

Modified feature: OSPF performance optimization

Modified feature: POS terminal access

Modified feature: License

Modified feature: IP performance optimization

Modified feature: AAA

Modified feature: Configuring a cellular interface for a 3G/4G modem

Modified feature: QoS on VXLAN tunnel interfaces

Modified feature: Option 60 encapsulation in DHCP replies

Modified feature: MPLS QoS support for matching the EXP field

Modified feature: MPLS QoS support for marking the EXP field

Modified feature: Automatic configuration

Modified feature: User profile

Modified feature: Default size of the TCP receive and send buffer

Modified feature: Obtaining fan and power module vendor information

Modified feature: Support for per-packet load sharing

Modified feature: Default user role

Modified feature: Debugging

Modified feature: SSH username

Modified feature: IS-IS hello packet sending interval

Modified feature: MP-group interface numbering

Modified feature: Setting the global link-aggregation load-sharing mode

Modified feature: 802.1X redirect URL

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Modified feature: Saving, rolling back, and loading the configuration

Modified feature: Displaying information about SSH users

Modified feature: SIP trusted nodes

Modified feature: IPsec ESP encryption algorithms

Modified feature: IPsec ESP authentication algorithms

Modified feature: IPsec AH authentication algorithms

Modified feature: Specifying an encryption algorithm for an IKE proposal

Modified feature: Specifying an authentication algorithm for an IKE proposal

Modified feature: Generating asymmetric key pairs

Modified feature: Specifying an ECDSA key pair for certificate request

Modified feature: Setting the electrical impedance

Modified feature: POS access statistics, SNMP notifications for POS access, and NII

Modified feature: QoS MIB

Modified feature: Enabling PFS for an IPsec transform set

Removed feature: Tiny proxy

Removed feature: Displaying switching fabric channel usage

New feature: Support of multicast for ADVPN

Configuring support of multicast for ADVPN

For information about this feature, see IPv4/IPv6 PIM and IPv4/IPv6 multicast routing and forwarding in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide*.

Command reference

The following commands were added:

- **display ipv6 pim nbma-link.**
- **display pim nbma-link.**
- **ipv6 pim nbma-mode.**
- **pim nbma-mode.**

ADVPN multicast parameters were added to the following commands:

- **display ipv6 multicast forwarding df-info.**
- **display ipv6 multicast forwarding-table.**
- **display ipv6 multicast routing-table.**
- **display ipv6 pim df-info.**
- **display ipv6 pim routing-table.**
- **display multicast forwarding df-info.**
- **display multicast forwarding-table.**
- **display multicast routing-table.**
- **display pim df-info.**
- **display pim routing-table.**

For information about the commands, see IPv4/IPv6 PIM and IPv4/IPv6 multicast routing and forwarding commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference*.

New feature: Application layer state filtering

Configuring application layer state filtering

For information about this feature, see ASPF in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following keywords were added to the **detect** command:

- **dns.**
- **http.**
- **smtp.**
- **action.**
- **drop.**

The fields that indicate application layer status were added to the output from the **display aspf policy** command.

For information about the commands, see ASPF in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: SIP keepalive

Configuring SIP keepalive

You can configure in-dialog keepalive and out-of-dialog keepalive.

Command reference

New command: options-ping

Use **options-ping** to globally enable in-dialog keepalive.

Use **undo options-ping** to globally disable in-dialog keepalive.

Syntax

options-ping *seconds*

undo options-ping

Default

In-dialog keepalive is disabled globally.

View

SIP view

Predefined use roles

network-admin

Parameters

seconds: Specifies the global interval for sending OPTIONS messages during a session, in the range of 60 to 1200 seconds.

Usage guidelines

This command enables the device to periodically send OPTIONS messages at the specified interval to monitor the status of the remote SIP UA during a session. It does not take effect when the session refresh negotiation succeeds before a call is established.

If you disable this feature, the device does not send OPTIONS messages after a call is established.

Example

```
# Globally enable in-dialog keepalive and set the interval to 60 seconds for sending OPTIONS messages during a session.
```

```
<Sysname> system-view
```

```
[Sysname] voice-setup
```

```
[Sysname-voice] sip
```

```
[Sysname-voice-sip] options-ping 60
```

New command: voice-class sip options-ping

Use **voice-class sip options-ping** to enable in-dialog keepalive for a VoIP entity.

Use **voice-class sip options-ping** to disable in-dialog keepalive for a VoIP entity.

Syntax

```
voice-class sip options-ping { global | seconds }
```

```
undo voice-class sip options-ping
```

Default

A VoIP entity uses the global configuration for in-dialog keepalive.

Views

VoIP entity view

Predefined user roles

network-admin

Parameters

global: Applies the global configuration for in-dialog keepalive to the VoIP entity.

seconds: Specifies the interval for sending OPTIONS messages during a session, in the range of 60 to 1200 seconds.

Usage guidelines

For a VoIP entity, the entity-specific in-dialog keepalive interval takes priority over the global in-dialog keepalive interval set in SIP view.

Examples

```
# Enable in-dialog keepalive for VoIP entity 1 and set the interval to 60 seconds for sending OPTIONS messages during a session.
```

```

<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip options-ping 60
# Apply the global configuration for in-dialog keepalive to VoIP entity 1.
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip options-ping global

```

New feature: Multicast fast forwarding

Configuring multicast fast forwarding

In this release, the router supports multicast fast forwarding.

Command reference

New command: display multicast fast-forwarding cache

Use **display multicast fast-forwarding cache** to display information about multicast fast forwarding entries.

Syntax

Centralized devices:

```
display multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache [ source-address | group-address ] *
```

Distributed devices in standalone mode: Centralized IRF devices:

```
display multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache [ source-address | group-address ] * [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache [ source-address | group-address ] * [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot slot-number: Specifies a card by its slot number. If you do not specify a card, this command displays multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast fast forwarding entries for the master device. (Centralized IRF devices.)

chassis chassis-number slot slot-number: Specifies a card on an IRF member device. The **chassis-number** argument represents the member ID of the IRF member device. The **slot-number** argument represents the slot number of the card. If you do not specify a card, this command displays multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

Display multicast fast forwarding entries on the public network.

```
<Sysname> display multicast fast-forwarding cache
Total 1 entries, 1 matched
(60.1.1.200, 225.0.0.2)
Status : Enabled
Source port: 2001 Destination port: 2002
Protocol : 2 Flag : 0x2
Incoming interface: GigabitEthernet1/0/3
List of 1 outgoing interfaces:
GigabitEthernet1/0/2
Status: Enabled Flag: 0x14
```

Table 1 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the multicast fast forwarding table, and the total number of matching (S, G) entries.
(60.1.1.200, 225.0.0.2)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • 0x1—The entry is created because of packets passed through between cards. • 0x2—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • 0x1—The interface is added to the entry because of packets passed through between cards. • 0x2—The interface is added to an existing entry. • 0x4—The MAC address of the interface is needed for fast forwarding. • 0x8—The interface is an outgoing interface associated with the incoming VLAN or super VLAN interface. • 0x10—The interface is associated with the entry. • 0x20—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • Enabled—Available.

Field	Description
	Disabled—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

New command: reset multicast fast-forwarding cache

Use **reset multicast fast-forwarding cache** to clear multicast fast forwarding entries.

Syntax

Centralized devices:

```
reset multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache { { source-address | group-address } * | all }
```

Distributed devices in standalone mode: Centralized IRF devices:

```
reset multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache { { source-address | group-address } * | all } [ slot slot-number ]
```

Distributed devices in IRF mode:

```
reset multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache { { source-address | group-address } * | all } [ chassis chassis-number slot slot-number ]
```

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears multicast fast forwarding entries for the master device. (Centralized IRF devices.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command clears multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

Clear all multicast fast forwarding entries on the public network.

```
<Sysname> reset multicast fast-forwarding cache all
```

Clear the multicast fast forwarding entry for multicast source and group (20.0.0.2, 225.0.0.2) on the public network.

```
<Sysname> reset multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

New command: display ipv6 multicast fast-forwarding cache

Use **display ipv6 multicast fast-forwarding cache** to display information about IPv6 multicast fast forwarding entries.

Syntax

Centralized devices:

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache  
[ ipv6-source-address | ipv6-group-address ] *
```

Distributed devices in standalone mode: Centralized IRF devices:

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache  
[ ipv6-source-address | ipv6-group-address ] * [ slot slot-number ]
```

Distributed devices in IRF mode:

```
display ipv6 multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache  
[ ipv6-source-address | ipv6-group-address ] * [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers from 0 to F.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays IPv6 multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast fast forwarding entries for the master device. (Centralized IRF devices.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command displays IPv6 multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

Display IPv6 multicast fast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast fast-forwarding cache
```

```
Total 1 entries, 1 matched
```

```
(FE1F:60::200, FF0E::1)
```

```
Status      : Enabled
```

```
Source port: 2001
```

```
Destination port: 2002
```

```

Protocol      : 2                               Flag      : 0x2
Incoming Interface: GigabitEthernet1/0/3
List of 1 outgoing interfaces:
GigabitEthernet1/0/2
Status: Enabled                               Flag: 0x14

```

Table 2 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the IPv6 multicast fast forwarding table, and the total number of matching (S, G) entries.
(FE1F:60::200, FF0E::1)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • 0x1—The entry is created because of packets passed through between cards. • 0x2—The entry is added by IPv6 multicast forwarding. The following flags are available for an outgoing interface: • 0x1—The interface is added to the entry because of packets passed through between cards. • 0x2—The interface is added to an existing entry. • 0x4—The MAC address of the interface is needed for fast forwarding. • 0x8—The interface is an outgoing interface associated with the incoming VLAN or super VLAN interface. • 0x10—The interface is associated with the entry. • 0x20—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • Enabled—Available. • Disabled—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

New command: reset ipv6 multicast fast-forwarding cache

Use **reset ipv6 multicast fast-forwarding cache** to clear IPv6 multicast fast forwarding entries.

Syntax

Centralized devices:

```
reset ipv6 multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache
{ { ipv6-source-address | ipv6-group-address } * | all }
```

Distributed devices in standalone mode: Centralized IRF devices:

```
reset ipv6 multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache
{ { ipv6-source-address | ipv6-group-address } * | all } [ slot slot-number ]
```

Distributed devices in IRF mode:

```
reset ipv6 multicast [ vpn-instance vpn-instance-name ] fast-forwarding cache
{ { ipv6-source-address | ipv6-group-address } * | all } [ chassis chassis-number slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers from 0 to F.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears IPv6 multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 multicast fast forwarding entries for the master device. (Centralized IRF devices.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. If you do not specify a card, this command clears IPv6 multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

Clear all IPv6 multicast fast forwarding entries on the public network

```
<Sysname> reset ipv6 multicast fast-forwarding cache all
```

Clear the IPv6 multicast fast forwarding entry for IPv6 multicast source and group (FE1F:20::2, FF0E::1) on the public network.

```
<Sysname> reset ipv6 multicast fast-forwarding cache felf:20::2 ff0e::1
```

New feature: SSL support for POS terminal access

Configuring an SSL policy for POS terminal access

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a TCP access POS terminal template.	posa terminal <i>terminal-id</i> type tcp listen-port <i>port</i> [idle-time <i>time</i>] [https ssl]	By default, no TCP access POS terminal templates exist.

Step	Command	Remarks
3. Specify an SSL server policy for TCP-based POS terminal templates.	posa terminal ssl-server-policy <i>policy-name</i>	By default, no SSL server policy is specified for TCP-based POS terminal templates. Execute this command if you specify the https or ssl keyword of the posa terminal command. The device uses the SSL server policy parameters to establish HTTPS or SSL connections with POS terminals.

Command reference

New command: posa terminal ssl-server-policy

Use **posa terminal ssl-server-policy** to specify an SSL server policy for TCP-based POS terminal templates.

User **undo posa terminal ssl-server-policy** to restore the default.

Syntax

posa terminal ssl-server-policy *policy-name*

undo posa terminal ssl-server-policy

Default

No SSL server policy is specified for TCP-based POS terminal templates.

Views

System view

Predefined user roles

network-admin

mdc-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

Execute this command if you specify the **https** or **ssl** keyword of the **posa terminal** command. The device uses the SSL server policy parameters to establish HTTPS or SSL connections with POS terminals.

Examples

Specify SSL server policy **policy1** for TCP-based POS terminal templates.

```
<Sysname> system-view
```

```
[Sysname] posa terminal ssl-server-policy policy1
```

Modified command: posa terminal

Old syntax

posa terminal *terminal-id* **type tcp** **listen-port** *port* [**idle-time** *time*]

Old syntax

posa terminal *terminal-id* **type tcp** **listen-port** *port* [**idle-time** *time*] [**https** | **ssl**]

Views

System view

Change description

The **https** and **nii** keywords were added. The router can use HTTPS or SSL connections to communicate with POS terminals.

New feature: Attack defense policy application to a security zone

Applying an attack defense policy to a security zone

To apply an attack defense policy to a security zone:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter security zone view.	security-zone name <i>Trust</i>	N/A
3. Apply an attack defense policy to the security zone.	attack-defense apply policy <i>policy-number</i>	By default, a security zone has no attack defense policy applied.

Command reference

The following commands were newly added:

- **attack-defense apply policy**
- **blacklist enable**
- **client-verify dns enable**
- **client-verify http enable**
- **client-verify tcp enable**
- **display attack-defense flood statistics ip**
- **display attack-defense flood statistics ipv6**
- **display attack-defense scan attacker ip**
- **display attack-defense scan attacker ipv6**
- **display attack-defense scan attacker ipv6**
- **display attack-defense scan victim ipv6**

- **display attack-defense statistics security-zone**
- **reset attack-defense statistics security-zone**

For information about the commands, see attack defense commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: AAA support for IKE extended authentication

Configuring IKE extended authentication

For information about this feature, see AAA configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **authentication ike** command was newly added.

The **ike** keyword was added to the **display local-user**, **undo local-user**, **service-type**, and **undo service-type** commands.

For information about the commands, see AAA commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Percentage-based CAR

Configuring percentage-based CAR

For information about this feature, see QoS in *H3C MSR Router Series Comware 7 ACL and QoS Configuration Guide*.

Command reference

The **percent car** command was added.

For information about the command, see traffic behavior commands in *H3C MSR Router Series Comware 7 ACL and QoS Command Reference*.

New feature: Logging OSPF router ID conflict events

Logging OSPF router ID conflict events

For information about this feature, see OSPF configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide*.

Command reference

The following commands were newly added:

- **database-filter peer** (OSPF view)
- **ospf database-filter**
- **ospf ttl-security**
- **ttl-security**

For information about the commands, see OSPF commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: AFT

Configuring AFT

For information about this feature, see AFT in *H3C MSR Router Series Comware 7 Layer 3—IP Services Configuration Guide*.

Command reference

For information about the commands, see AFT commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Configuring enhanced CC authentication in FIPS mode

Configuring enhanced CC authentication in FIPS mode

For information about this feature, see IPsec, SSH, SSL, and public key management in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **ecdsa** keyword was added to the following commands:

- **scp**.
- **scp ipv6**.
- **sftp**.
- **sftp ipv6**.
- **ssh2**.
- **ssh2 ipv6**.

The **dhe_rsa_aes_128_cbc_sha** and **dhe_rsa_aes_256_cbc_sha** keywords were removed from the **ciphersuite** command in FIPS mode.

The **secp192r1** and **secp256r1** keywords were added to the **public-key local create** command.

The **public-key local export ecdsa** command was added.

For more information about these commands, see IPsec, SSH, SSL, and public key management commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Support of AAA for NETCONF

Configuring support of AAA for NETCONF

For information about this feature, see AAA in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **radius session-control client** command was newly added. The **security-policy-server** command was deleted.

For information about the command, see AAA commands in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

New feature: Mobile IP tunnel interface settings

Configuring the mobile IP tunnel interface settings

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the mobile router feature and enter mobile router view.	ip mobile router	By default, the mobile router feature is disabled.
3. Assign a home address to the mobile router.	address <i>ip-address</i>	By default, the mobile router does not have any home addresses.
4. Specify the IP address of the home agent for the mobile router.	home-agent <i>ip-address</i>	By default, no home agent is specified for the mobile router.
5. (Optional.) Set the MTU for the mobile IP tunnel interface.	tunnel mtu <i>value</i>	By default, the MTU for the tunnel interface is 64000 bytes.
6. (Optional.) Set the DF bit to 0 for outgoing tunneled packets.	ip df-bit zero	By default, the DF bit of outgoing tunneled packets is not set.
7. (Optional.) Apply an IPsec policy to the mobile IP tunnel interface.	ipsec policy <i>policy-name</i>	By default, no IPsec policy is applied to the mobile IP tunnel interface.
8. (Optional.) Set the TCP MSS for the mobile IP tunnel interface.	tcp mss <i>value</i>	By default, no TCP MSS is set.

Command reference

The following commands were added:

- **ip df-bit zero**
- **ipsec policy**
- **tcp mss**

For information about the commands, see NEMO commands in *H3C MSR Router Series Comware 7 NEMO Command Reference*.

New feature: LISP

Configuring LISP

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

For information about the commands, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: LISP tunnel entries and dynamic mobility

Configuring LISP tunnel entries and dynamic mobility

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

For information about the commands, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: Support of IPv6 multicast routing for VPN instances

Enabling support of IP multicast routing for VPN instances

For information about this feature, see IPv6 multicast routing and forwarding in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide*.

Command reference

The **ipv6 multicast routing vpn-instance** command was added.

For information about the command, see IPv6 multicast routing and forwarding commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference*.

New feature: IPv4/IPv6 PIM NSR

Enabling IPv4/IPv6 PIM NSR

For information about this feature, see IPv4/IPv6 PIM in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide*.

Command reference

The **pim non-stop-routing** and **ipv6 pim non-stop-routing** commands were added.

For information about the commands, see IPv4/IPv6 PIM commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference*.

New feature: IGMP/MLD NSR

Enabling IGMP/MLD NSR

For information about this feature, see IGMP/MLD in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide*.

Command reference

The **igmp non-stop-routing** and **mld non-stop-routing** commands were added.

For information about the commands, see IGMP/MLD commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference*.

New feature: IPv4/IPv6 PIM passive mode

Enabling IPv4/IPv6 PIM passive mode

For information about this feature, see IPv4/IPv6 PIM in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide*.

Command reference

The **pim passive** and **ipv6 pim passive** commands were added.

For information about the commands, see IPv4/IPv6 PIM commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference*.

New feature: LISP virtual machine multi-hop mobility and DDT

Configuring LISP virtual machine multi-hop mobility and DDT

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

The **eid-notify** command was newly added.

For information about the command, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: LISP NSR

Configuring LISP NSR

The **display system internal lisp forwarding statistics** command was added. You can use the command to display the LISP thread statistics.

The **display system internal lisp nsr no-cache** command was added. You can use the command to display the tentative entries created during the NSR active/standby switchover.

The **display system internal lisp nsr status** command was added. You can use the command to display the LISP NSR status.

Command reference

The following commands were newly added:

- **display system internal lisp forwarding statistics**
- **display system internal lisp nsr no-cache**
- **display system internal lisp nsr status**

For information about the commands, see LISP probe commands in *H3C MSR Router Series Comware 7 Probe Command Reference*.

New feature: PPPoE client support for IPv6

Associating a dial rule with a dialup interface

For information about this feature, see DDR in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Configuration Guide*.

Command reference

The **ipv6** keyword is added to the **dialer-group rule** command. For information about this command, see DDR commands in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Command Reference*.

Specifying an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address

For information about this feature, see IPv6 basics in *H3C MSR Router Series Comware 7 Layer 3—IP Services Configuration Guide*.

Command reference

The **ipv6 address** command is added. For information about the command, see IPv6 basics commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Frame-Relay-related functions

Configuring multilink Frame Relay

For information about this feature, see multilink Frame Relay in *H3C MSR Router Series Comware 7 WAN Access Configuration Guide*.

Command reference

For information about the commands, see multilink Frame Relay commands in *H3C MSR Router Series Comware 7 WAN Access Command Reference*.

Configuring Frame Relay FRF.12 fragmentation

For information about this feature, see Frame Relay in *H3C MSR Router Series Comware 7 WAN Access Configuration Guide*.

Command reference

The following commands were added:

- **display fr fragment.**
- **fr fragment enable.**
- **fr fragment size.**

For information about the commands, see Frame Relay commands in *H3C MSR Router Series Comware 7 WAN Access Command Reference*.

Configuring Frame Relay STAC compression

For information about this feature, see Frame Relay in *H3C MSR Router Series Comware 7 WAN Access Configuration Guide*.

Command reference

The **display fr compression stac** and **fr compression stac enable** commands were added.

For information about the commands, see Frame Relay commands in *H3C MSR Router Series Comware 7 WAN Access Command Reference*.

Configuring Frame Relay IPv6 address mapping

For information about this feature, see Frame Relay in *H3C MSR Router Series Comware 7 WAN Access Configuration Guide*.

Command reference

The following commands were added:

- **display fr ipv6 map.**
- **fr ipv6 ind.**
- **fr map ipv6.**
- **fr ipv6 ind holdtime.**
- **fr ipv6 ind solicitation retrans-timer.**
- **reset fr ipv6 ind.**

For information about the commands, see Frame Relay commands in *H3C MSR Router Series Comware 7 WAN Access Command Reference*.

Enabling SNMP notifications for Frame Relay

For information about this feature, see Frame Relay in *H3C MSR Router Series Comware 7 WAN Access Configuration Guide*.

Command reference

The **snmp-agent trap enable fr** command was added.

For information about the command, see Frame Relay commands in *H3C MSR Router Series Comware 7 WAN Access Command Reference*.

Setting the Frame Relay interface type

For information about this feature, see Frame Relay in *H3C MSR Router Series Comware 7 WAN Access Configuration Guide*.

Command reference

The **fr interface-type** command was added.

For information about the command, see Frame Relay commands in *H3C MSR Router Series Comware 7 WAN Access Command Reference*.

Configuring Frame Relay QoS

For information about this feature, see FR QoS in *H3C MSR Router Series Comware 7 ACL and QoS Configuration Guide*.

Command reference

All commands were newly added.

For information about the commands, see FR QoS commands in *H3C MSR Router Series Comware 7 ACL and QoS Command Reference*.

New feature: DPI engine and content filtering

Configuring the DPI engine and content filtering

For information about this feature, see DPI overview and DPI engine in *H3C MSR Router Series Comware 7 DPI Configuration Guide*.

Command reference

For information about the commands, see DPI overview and DPI engine commands in *H3C MSR Router Series Comware 7 DPI Command Reference*.

New feature: IPS

Configuring IPS

For information about this feature, see IPS configuration in *H3C MSR Router Series Comware 7 DPI Configuration Guide*.

Command reference

For information about the commands, see IPS commands in *H3C MSR Router Series Comware 7 DPI Command Reference*.

New feature: NBAR

Configuring NBAR

For information about this feature, see APR in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following new commands were added:

- **apr signature update.**
- **Description.**
- **Destination.**
- **Direction.**
- **Disable.**
- **display app-group.**
- **display application.**
- **display apr signature information.**
- **include app-group.**
- **nbar application.**

- **nbar protocol-discovery.**
- **service-port.**
- **signature.**
- **source.**

For information about the commands, see APR in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: URL filtering

Configuring URL filtering

For information about this feature, see URL filtering configuration in *H3C MSR Router Series Comware 7 DPI Configuration Guide*.

Command reference

For information about the commands, see URL filtering commands in *H3C MSR Router Series Comware 7 DPI Command Reference*.

New feature: Local portal Web server

Configuring a local portal Web server

For information about this feature, see portal in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following commands were added:

- **portal local-web-server**
- **default-logon-page**
- **logon-page**
- **tcp-port**

The **ssid** keyword was added to the **url-parameter** *param-name* { **apmac** | **original-url** | **source-address** | **source-mac** | **ssid** | **value expression** } command.

For information about the commands, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Support of portal for NETCONF

Support for NETCONF was added to portal.

New feature: Newly-added MIB objects

Event MIB added support for the hh3cWirelessCardModemMode and hh3cWirelessCardCurNetConn MIB objects.

New feature: Performing a loopback test

Performing a loopback test

For information about this feature, see WAN interface configuration in *H3C MSR Router Series Comware 7 Interface Configuration Guide*.

Command reference

New command: loopback-test

For information about the command, see WAN interface commands in *H3C MSR Router Series Comware 7 Interface Command Reference*.

New feature: IPS, ACG, and SSL VPN licenses

This release added support for IPS, ACG and SSL VPN licenses.

New feature: Support of NQA for NETCONF

Support for NETCONF was added to NQA.

New feature: Configuring CWMP to support VPN

Configuring CWMP to support VPN

For information about this feature, see CWMP configuration in *H3C MSR Router Series Comware 7 Network Management and Monitoring Configuration Guide*.

Command reference

For information about the commands, see CWMP commands in *H3C MSR Router Series Comware 7 Network Management and Monitoring Command Reference*.

New feature: Transceiver module source alarm

Disabling transceiver module source alarm

For information about this feature, see device management in *H3C MSR Router Series Comware 7 Fundamentals Configuration Guide*.

Command reference

transceiver phony-alarm-disable

For information about this command, see device management commands in *H3C MSR Router Series Comware 7 Fundamentals Command Reference*.

New feature: VLAN interface performance optimization

This software version optimized the following items:

- VLAN functions used for sending data in the adaption layer.
- Processing flow of the RAW functions for sending and receiving data for chips mv88ex, mvcps, and bcm5614x.

New feature: POSA

POSA terminal access configuration

For information about this feature, see POS terminal access in *H3C MSR Router Series Comware 7 Terminal Access Configuration Guide*.

POS terminal access command reference

The following commands were added:

- **reset posa statistics nii**
- **display posa statistics nii**
- **trade-exchanges**
- **posa trade-falling-threshold**
- **display posa statistics caller-id**
- **posa e1-dial-falling-threshold**
- **snmp-agent trap enable posa**
- **display posa statistics caller-ip**

For information about the commands, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New feature: Specifying a backup processing slot for an interface

Specifying a backup processing slot for an interface

For information about this feature, see the configuration guides for the following modules:

- PPP, L2TP, HDLC, and DDR in *H3C MSR Router Series Layer 2—WAN Access Configuration Guide*.
- Ethernet link aggregation in *H3C MSR Router Series Layer 2—LAN Switching Configuration Guide*.
- MPLS protection switching in *H3C MSR Router Series MPLS Configuration Guide*.

Command reference

The **service standby** command was added to support this feature.

For information about this command, see the command references for the following modules:

- PPP, L2TP, HDLC, and DDR in *H3C MSR Router Series Layer 2—WAN Access Command Reference*.
- Ethernet link aggregation in *H3C MSR Router Series Layer 2—LAN Switching Command Reference*.
- MPLS protection switching in *H3C MSR Router Series Command Reference*.

New feature: Configuring the ISDN leased line

Configuring the ISDN leased line

For information about this feature, see ISDN configuration in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Configuration Guide*.

Command reference

Support for the **isdn leased-line** command was added.

For information about the command, see ISDN commands in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Command Reference*.

New feature: NAT support for multicast source address in PIM join/prune packets

This feature enables the device to act as a NAT gateway and perform NAT on the multicast source address in PIM join or prune packets based on NAT mappings. Use this feature in a multicast scenario where the multicast source resides on a private network, multicast receivers reside on private networks, and PIM-SSM mode is used.

New feature: GDOI GM group anti-replay window

Configuring the anti-replay window for a GDOI GM group

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a GDOI GM group and enter GDOI GM group view.	gdoi gm group [ipv6] <i>group-name</i>	By default, no GDOI GM groups exist.
3. (Optional.) Set the anti-replay window size for the GDOI GM group.	client anti-replay window { sec <i>seconds</i> msec <i>milliseconds</i> }	By default, the anti-replay window size is not set for a GDOI GM group.

Command reference

client anti-replay window

Use **client anti-replay window** to set the anti-replay window size for a GDOI GM group.

Use **undo client anti-replay window** to restore the default.

Syntax

client anti-replay window { **sec** *seconds* | **msec** *milliseconds* }

undo client anti-replay window

Default

The anti-replay window size is not set for a GDOI GM group.

Views

GDOI GM group view

Predefined user roles

network-admin

Parameters

sec *seconds*: Specifies the anti-replay window size in seconds in the range of 1 to 100.

msec *milliseconds*: Specifies the anti-replay window size in milliseconds in the range of 100 to 10000.

Usage guidelines

The anti-replay window size set in this command takes priority over the anti-replay window size obtained from the KS. If you do not configure this command, the anti-replay window size obtained from the KS is used.

This command must be used together with the Cisco IP-D3P feature.

Examples

```
# Set the anti-replay window size to 50 seconds for GDOI GM group group1.
```

```
<Sysname> system-view
```

```
[Sysname] gdoi gm group group1
```

```
[Sysname-gdoi-gm-group-group1] client anti-replay window sec 50
```

New feature: SIP compatibility

Configuring SIP compatibility

If a third-party device does not implement SIP in strict accordance with the RFC standard, you can configure SIP compatibility for the router to interoperate with the third-party device.

With the **sip-compatible t38** command configured, the router excludes :0 from the following SDP parameters in the originated re-INVITE messages:

- T38FaxTranscodingJBIG.
- T38FaxTranscodingMMR.
- T38FaxFillBitRemoval.

With the **sip-compatible x-param** command configured, the router adds SDP description information (a=X-fax and a=X-modem) for fax pass-through and modem pass-through in the originated re-INVITE messages.

To configure SIP compatibility:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter voice view.	voice-setup	N/A
3. Enter SIP view.	sip	N/A
4. Configure SIP compatibility.	sip-compatible { t38 x-param }	By default, SIP compatibility is not configured.

Command reference

New command:sip-compatible

Use **sip-compatible** to configure SIP compatibility with a third-party device.

Use **undo sip-compatible** to restore the default.

Syntax

sip-compatible { t38 | x-param }

undo sip-compatible { t38 | x-param }

Default

SIP compatibility is not configured.

Views

SIP view

Predefined user roles

network-admin

Parameters

t38: Configures SIP compatibility for standard T.38 fax. With this keyword specified, the router excludes :0 from the following SDP parameters in the originated re-INVITE messages:

- T38FaxTranscodingJBIG.
- T38FaxTranscodingMMR.
- T38FaxFillBitRemoval.

This keyword is required when the router interoperates with a third-party softswitch device to exchange T.38 fax messages.

x-param: Configures SIP compatibility for fax pass-through and modem pass-through. With this keyword specified, the router adds SDP description information for fax pass-through and modem pass-through to outgoing re-INVITE messages. This keyword is required when the router interoperates with a third-party softswitch device to perform fax pass-through and modem pass-through.

Usage guidelines

The **t38** and **x-param** keywords can be both configured to interoperate with a third-party softswitch device.

Examples

Configure SIP compatibility for standard T.38 fax.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
```

New feature: Voice VLAN

Configuring a voice VLAN

Configuring a port to operate in automatic voice VLAN assignment mode

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Set the voice VLAN aging timer.	voice-vlan aging <i>minutes</i>	By default, the aging timer of a voice VLAN is 1440 minutes.
3. (Optional.) Enable the voice VLAN security mode.	voice-vlan security enable	By default, the voice VLAN security mode is enabled.
4. (Optional.) Add an OUI address for voice packet identification.	voice-vlan mac-address <i>oui mask</i> <i>oui-mask</i> [description <i>text</i>]	By default, system default OUI addresses exist.
5. Enter interface view.	- Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> - Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> - Enter S-channel interface view: interface s-channel <i>interface-number.channel-id</i> - Enter S-channel aggregate interface view: interface schannel-aggregation <i>interface-number.channel-id</i> - Enter Layer 2 RPR logical interface view: interface rpr-bridge <i>interface-number</i>	N/A
6. Set the link type of the port.	- Set the port link type to trunk: port link-type trunk - Set the port link type to hybrid: port link-type hybrid	N/A
7. Configure the port to operate in automatic voice VLAN assignment mode.	voice-vlan mode auto	By default, the automatic voice VLAN assignment mode is enabled.

Step	Command	Remarks
8. Enable the voice VLAN feature on the port.	voice-vlan <i>vlan-id</i> enable	By default, the voice VLAN feature is disabled on a port. Before you execute this command, make sure the specified VLAN already exists.

Configuring a port to operate in manual voice VLAN assignment mode

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Enable the voice VLAN security mode.	voice-vlan security enable	By default, the voice VLAN security mode is enabled.
3. (Optional.) Add an OUI address for voice packet identification.	voice-vlan mac-address <i>oui</i> <i>mask</i> <i>oui-mask</i> [description <i>text</i>]	By default, system default OUI addresses exist.
4. Enter interface view.	- Enter Layer 2 Ethernet interface view: interface <i>interface-type</i> <i>interface-number</i> - Enter Layer 2 aggregate interface view: interface bridge-aggregation <i>interface-number</i> - Enter S-channel interface view: interface s-channel <i>interface-number.channel-id</i> - Enter S-channel aggregate interface view: interface schannel-aggregation <i>interface-number:channel-id</i> - Enter Layer 2 RPR logical interface view: interface rpr-bridge <i>interface-number</i>	N/A
5. Configure the port to operate in manual voice VLAN assignment mode.	undo voice-vlan mode auto	By default, a port operates in automatic voice VLAN assignment mode.
6. Set the link type of the port.	- Set the port link type to access: port link-type access - Set the port link type to trunk: port link-type trunk - Set the port link type to hybrid: port link-type hybrid	By default, each port is an access port.

Step	Command	Remarks
7. Assign the access, trunk, or hybrid port to the voice VLAN.	- For the access port: port access vlan <i>vlan-id</i> - For the trunk port: port trunk permit vlan { <i>vlan-id-list</i> all } - For the hybrid port: port hybrid vlan <i>vlan-id-list</i> { tagged untagged }	After you assign an access port to the voice VLAN, the voice VLAN becomes the PVID of the port.
8. (Optional.) Configure the voice VLAN as the PVID of the trunk or hybrid port.	- For the trunk port: port trunk pvid vlan <i>vlan-id</i> - For the hybrid port: port hybrid pvid vlan <i>vlan-id</i>	This step is required for untagged incoming voice traffic and prohibited for tagged incoming voice traffic.
9. Enable the voice VLAN feature on the port.	voice-vlan <i>vlan-id</i> enable	By default, the voice VLAN feature is disabled on a port. Before you execute this command, make sure the specified VLAN already exists.

Enabling LLDP for automatic IP phone discovery

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable LLDP for automatic IP phone discovery.	voice-vlan track lldp	By default, LLDP for automatic IP phone discovery is disabled.

Configuring LLDP to advertise a voice VLAN

For IP phones that support LLDP, the device advertises the voice VLAN information to the IP phones through LLDP-MED TLVs.

To configure LLDP to advertise a voice VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
3. Configure an advertised voice VLAN ID.	lldp tlv-enable med-tlv network-policy <i>vlan-id</i>	By default, no advertised voice VLAN ID is configured.

Configuring CDP to advertise a voice VLAN

If an IP phone supports CDP but does not support LLDP, it sends CDP packets to the device to request the voice VLAN ID. If the IP phone does not receive the voice VLAN ID within a time period,

it sends out untagged voice packets. These untagged voice packets cannot be differentiated from other types of packets.

You can configure CDP compatibility on the device to enable it to perform the following operations:

- Receive and identify CDP packets from the IP phone.
- Send CDP packets to the IP phone. The voice VLAN information is carried in the CDP packets.

After receiving the advertised VLAN information, the IP phone starts automatic voice VLAN configuration. Packets from the IP phone will be transmitted in the dedicated voice VLAN.

To configure CDP to advertise a voice VLAN:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable CDP compatibility.	lldp compliance cdp	By default, CDP compatibility is disabled.
3. Enter Layer 2 Ethernet interface view.	interface <i>interface-type</i> <i>interface-number</i>	N/A
4. Configure CDP-compatible LLDP to operate in TxRx mode.	lldp compliance admin-status cdp txrx	By default, CDP-compatible LLDP operates in disable mode.
5. Configure an advertised voice VLAN ID.	cdp voice-vlan <i>vlan-id</i>	By default, no advertised voice VLAN ID is configured.

Displaying and maintaining voice VLANs

Execute **display** commands in any view.

Task	Command
Display the voice VLAN state.	display voice-vlan state
Display OUI addresses on a device.	display voice-vlan mac-address

Command reference

The following commands were added:

- **display voice-vlan mac-address.**
- **display voice-vlan state.**
- **voice-vlan aging.**
- **voice-vlan enable.**
- **voice-vlan mac-address.**
- **voice-vlan mode auto.**
- **voice-vlan security enable.**

- **voice-vlan track lldp.**

For more information about these commands, see *H3C MSR Series Routers Layer 2—LAN Switching Command Reference(V7)*.

New feature: L2TP-based EAD

Enabling L2TP-based EAD

EAD authenticates PPP users that pass the access authentication. PPP users that pass EAD authentication can access network resources. PPP users that fail EAD authentication can only access the resources in the quarantine areas.

EAD uses the following procedure:

1. The iNode client uses L2TP to access the LNS. After the client passes the PPP authentication, the CAMS/IMC server assigns isolation ACLs to the LNS. The LNS uses the isolation ACLs to filter incoming packets.
2. After the IPCP negotiation, the LNS sends the IP address of the CAMS/IMC server to the iNode client. The server IP address is permitted by the isolation ACLs.
3. The CAMS/IMC sever authenticates the iNode client and performs security check for the iNode client. If the iNode client passes security check, the CAMS/IMC server assigns security ACLs for the iNode client to the LNS. The iNode client can access network resources.

To enable L2TP-based EAD:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a VT interface and enter its view	interface virtual-template <i>virtual-template-number</i>	N/A
3. Enable L2TP-based EAD.	ppp access-control enable	By default, L2TP-based EAD is disabled.

Command reference

ppp access-control enable

Use **ppp access-control enable** to enable L2TP-based EAD.

Use **undo ppp access-control enable** to disable L2TP-based EAD.

Syntax

ppp access-control enable

undo ppp access-control enable

Default

L2TP-based EAD is disabled.

Views

VT interface view

Predefined user roles

network-admin

Usage guidelines

This command does not apply to VA interfaces that already exist in the VT interface. It only applies to newly created VA interfaces.

Different ACLs are required for different users if the VT interface is used as the access interface for the LNS.

After L2TP-based EAD is enabled, the LNS transparently passes CAMS/IMC packets to the iNode client to inform the client of EAD server information, such as the IP address.

Examples

```
# Enable L2TP-based EAD.
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] ppp access-control enable
```

display ppp access-control interface

Use **display ppp access-control interface** to display access control information for VA interfaces on a VT interface.

Syntax

display ppp access-control interface { *interface-type interface-number* | *interface-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

interface-name: Specifies an interface by its name.

Examples

```
# Display access control information for VA interfaces on VT interface 2.
<Sysname> display ppp access-control interface virtual-template 2
Interface: Virtual-Template2:0
```

```
User Name: mike
In-bound Policy: acl 3000
Totally 0 packets, 0 bytes, 0% permitted,
Totally 0 packets, 0 bytes, 0% denied.

Interface: Virtual-Template2:1
User Name: tim
In-bound Policy: acl 3001
Totally 0 packets, 0 bytes, 0% permitted,
Totally 0 packets, 0 bytes, 0% denied.
```

Table 3 Command output

Field	Description
Interface	VA interface that the PPP user accesses.
User Name	Username of the PPP user.
In-bound Policy	Security ACLs for the PPP user.
Totally x packets, x bytes, x% permitted	Total number, data rate, and pass percentage of permitted packets.
Totally x packets, x bytes, x% denied	Total number, data rate, and reject percentage of denied packets.

New feature: Configuring device poweroff alarming

This feature is available on an IPRAN device to detect a device poweroff event and issue a poweroff alarm by sending SNMP notifications or log messages.

Command reference

dying-gasp host

Use **dying-gasp host** to configure poweroff alarm destination host settings.

Use **undo dying-gasp host** to remove poweroff alarm destination host settings.

Syntax

```
dying-gasp host { ip-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] snmp-trap
version { v1 | v2c } securityname security-string
```

```
dying-gasp host { ip-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] syslog
```

```
undo dying-gasp host { ip-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
{ snmp-trap | syslog }
```

Default

No poweroff alarm destination host settings are configured.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IPv4 address of the destination host to which the device sends the poweroff alarm.

ipv6 ipv6-address: Specifies the IPv6 address of the destination host to which the device sends the poweroff alarm.

vpn-instance vpn-instance-name: Specifies the VPN instance to which the destination host belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the destination host belongs to the public network, do not specify this option.

snmp-trap: Uses an SNMP notification to send the poweroff alarm.

version: Specifies the SNMP version.

- **v1**: Uses SNMPv1.
- **v2c**: Uses SNMPv2c.

securityname security-string: Specifies an SNMPv1 or SNMPv2c community name, a string of 1 to 32 characters.

syslog: Uses a log message to send the poweroff alarm.

Usage guidelines

The device can send the poweroff alarm to multiple destination hosts at the same time. The maximum number of destination hosts depends on the device model.

Examples

Configure the device to send the poweroff alarm to the host at 1.1.1.1 by using an SNMPv1 notification. The community name is **public**.

```
<Sysname> system-view
[Sysname] dying-gasp host 1.1.1.1 snmp-trap version v1 securityname public
```

dying-gasp source

Use **dying-gasp source** to specify the source interface for sending the poweroff alarm.

Use **undo dying-gasp source** to restore the default.

Syntax

dying-gasp source *interface-type* { *interface-number* | *interface-number.subnumber* }

undo dying-gasp source

Default

No source interface is specified.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type { *interface-number* | *interface-number.subnumber* }: Specifies a Layer 3 interface or subinterface. The *interface-type* argument specifies the interface type. The *interface-number* argument specifies the interface number. The *subnumber* argument specifies the subinterface number and is in the range of 1 to 4094.

Usage guidelines

The device uses the IPv6 address or primary IPv4 address of the specified source interface as the source address for outgoing poweroff alarm packets. The destination hosts use this address to identify SNMP notifications or log messages received from the device.

If no IPv4 or IPv6 addresses are configured for the specified source interface, this command does not take effect. For this command to take effect, assign an IPv4 or IPv6 address to the source interface.

Examples

Use the interface Loopback 1 as the source interface for sending the poweroff alarm.

```
<Sysname> system-view  
[Sysname] dying-gasp source interface loopback1
```

display dying-gasp host

Use **display dying-gasp host** to display poweroff alarm destination host settings.

Syntax

display dying-gasp host

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display poweroff alarm destination host settings.

```
<sysname> display dying-gasp host
```

IPv4 address: 1.1.1.0
Message type: SNMP trap
Securityname: pl
Version: V1

IPv4 address: 1.1.1.1
Message type: Syslog

IPv6 address: 1::1
VPN instance: test
Message type: SNMP trap
Securityname: pl
Version: V1

IPv6 address: 1::1
VPN instance: test
Message type: Syslog

Table 4 Command output

Field	Description
IPv4 address	IPv4 address of the poweroff alarm destination host.
IPv6 address	IPv6 address of the poweroff alarm destination host.
VPN instance	VPN instance to which the poweroff alarm destination host belongs.
Message type	Message types that the poweroff alarm destination host supports: • SNMP Trap—SNMP notification. • Syslog—Log message.
Securityname	SNMPv1 or SNMPv2c community name. This field is displayed when the message type is SNMP Trap .
Version	SNMP version: • v1—SNMPv1. • v2c—SNMPv2c. This field is displayed when the message type is SNMP Trap .

New feature: BFD for an aggregation group

Enabling BFD for an aggregation group

BFD for Ethernet link aggregation can monitor member link status in an aggregation group. After you enable BFD on an aggregate interface, each Selected port in the aggregation group establishes a BFD session with its peer port. BFD operates differently depending on the aggregation mode.

- **BFD for static aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. The local port is placed in Unselected

state. The BFD session between the local and peer ports remains, and the local port keeps sending BFD packets. When the link is recovered, the local port receives BFD packets from the peer port, and BFD notifies the Ethernet link aggregation module that the peer port is reachable. The local port is placed in Selected state again. This mechanism ensures that the local and peer ports of a static aggregate link have the same aggregation state.

- **BFD for dynamic aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. BFD clears the session and stops sending BFD packets. When the link is recovered and the local port is placed in Selected state again, the local port establishes a new session with the peer port. BFD notifies the Ethernet link aggregation module that the peer port is reachable. Because BFD provides fast failure detection, the local and peer systems of a dynamic aggregate link can negotiate the aggregation state of their member ports faster.

For more information about BFD, see *H3C MSR Router Series Comware 7 High Availability Configuration Guide*.

Configuration restrictions and guidelines

When you enable BFD for an aggregation group, follow these restrictions and guidelines:

- Make sure the source and destination IP addresses are consistent at the two ends of an aggregate link. For example, if you execute **link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2** on the local end, execute **link-aggregation bfd ipv4 source 2.2.2.2 destination 1.1.1.1** on the peer end. The source and destination IP addresses cannot be the same.
- The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode.
- As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.
- Make sure the number of member ports in a BFD-enabled aggregation group is not larger than the number of BFD sessions supported by the device. Otherwise, this command might cause some Selected ports in the aggregation group to change to the Unselected state.

Configuration procedure

To enable BFD for an aggregation group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter Layer 3 aggregate interface view.	interface route-aggregation <i>interface-number</i>	N/A
3. Enable BFD for the aggregation group.	link-aggregation bfd ipv4 source <i>ip-address destination ip-address</i>	By default, BFD is disabled for an aggregation group. The source and destination IP addresses of BFD sessions must be unicast addresses excluding

Step	Command	Remarks
		0.0.0.0.

Command reference

link-aggregation bfd ipv4

Use **link-aggregation bfd ipv4** to enable BFD for an aggregation group.

Use **undo link-aggregation bfd** to disable BFD for an aggregation group.

Syntax

link-aggregation bfd ipv4 source *ip-address* **destination** *ip-address*

undo link-aggregation bfd

Default

BFD is disabled for an aggregation group.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

source *ip-address*: Specifies the unicast source IP address of BFD sessions. The source IP address cannot be 0.0.0.0.

destination *ip-address*: Specifies the unicast destination IP address of BFD sessions. The destination IP address cannot be 0.0.0.0.

Usage guidelines

Make sure the source and destination IP addresses are consistent at the two ends of an aggregate link. For example, if you execute **link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2** on the local end, execute **link-aggregation bfd ipv4 source 2.2.2.2 destination 1.1.1.1** on the peer end. The source and destination IP addresses cannot be the same.

The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode. For more information about BFD, see *H3C MSR Router Series Comware 7 High Availability Configuration Guide*.

As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.

Make sure the number of member ports in a BFD-enabled aggregation group is not larger than the number of BFD sessions supported by the device. Otherwise, this command might cause some Selected ports in the aggregation group to change to the Unselected state.

Examples

Enable BFD for Layer 3 aggregation group 1, and specify the source and destination IP addresses as 1.1.1.1 and 2.2.2.2 for BFD sessions.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2
```

New feature: 4G modem IMSI/SN binding authentication

This feature includes the IMSI/SN information in the 4G dial-up authentication information.

Command reference

apn

Use **apn** to create an access point name (APN).

Use **undo apn** to remove an APN.

Syntax

apn { dynamic | static *apn* }

undo apn

Default

No APN is configured.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

dynamic: Uses an APN automatically assigned by the service provider.

static *apn*: Specifies the APN provided by the service provider. It is a string of 1 to 100 characters. Whether the string is case-sensitive varies by service providers.

Usage guidelines

You must specify an APN for a 4G dial-up profile.

Examples

```
# Specify the APN apn1 for the 4G dial-up profile test.
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] apn static apn1
```

apn-profile

Use **apn-profile** to create a 4G dial-up profile.

Use **undo apn-profile** to remove a 4G dial-up profile.

Syntax

```
apn-profile profile-name
undo apn-profile profile-name
```

Default

No 4G dial-up profiles are configured.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a 4G dial-up profile name.

Usage guidelines

A 4G dial-up profile takes effect only after you associate the profile with a 4G interface. To remove a 4G dial-up profile, you must first remove the association between the profile and the 4G interface.

Examples

```
# Create the 4G dial-up profile test.
<Sysname> system-view
[Sysname] apn-profile test
```

apn-profile apply

Use **apn-profile apply** to specify a 4G dial-up profile.

Use **undo apn-profile apply** to restore the default.

Syntax

```
apn-profile apply profile-name [ backup profile-name ]
undo apn-profile apply
```

Default

No 4G dial-up profiles are specified.

Views

Eth-channel interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a primary 4G dial-up profile name.

backup *profile-name*: Specifies a backup 4G dial-up profile name.

Usage guidelines

After you specify a 4G dial-up profile for a 4G modem, the 4G modem uses the settings in the profile to negotiate with the service provider's device.

The primary profile always has priority over the backup profile. For each dialup connection establishment, the 4G modem uses the backup profile only when it has failed to dial up using the primary profile.

This command takes effect only on dialup connections initiated after the command is configured. It does not take effect on a dialup connection that has been established.

Examples

Specify the primary 4G dial-up profile **test** and the backup 4G dial-up profile **bktest** for Eth-channel interface 2/4/0:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 2/4/0:0
[Sysname-Eth-channel2/4/0:0] apn-profile apply test backup bktest
```

attach-format

Use **attach-format** to set a separator for the authentication information to be sent.

Use **undo attach-format** to restore the default.

Syntax

attach-format **imsi-sn** **split** *splitchart*

undo attach-format **imsi-sn** **split**

Default

No separator is set for the authentication information to be sent.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

split *splitchart*: Specifies a separator. It can be a letter, a digit, or a sign such as a percent sign (%) or a pound sign (#).

Usage guidelines

If IMSI/SN binding authentication is enabled, the IMSI/SN information is included in the authentication information in addition to the username. You need to configure a separator to separate different types of information. For example, if you specify the separator as #, the authentication information will be sent in the following format: *imsiinfo#sninfo#username*.

Examples

Configure the pound sign (#) as the separator for the authentication information to be sent.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] attach-format imsi-sn split #
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for a 4G dial-up profile.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode { **pap** | **chap** | **pap-chap** } **user** *user-name* **password** { **cipher** | **simple** } *password*

undo authentication-mode

Default

No authentication mode is configured for a 4G dial-up profile.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

chap: Specifies CHAP authentication.

pap: Specifies PAP authentication.

pap-chap: Specifies CHAP or PAP authentication.

user *username*: Specifies the username for authentication, a case-sensitive string of 1 to 32 characters.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

password: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters

Examples

Specify the CHAP authentication mode for the 4G dial-up profile **test**. Specify the CHAP authentication username as **user1** and the password as **123456**.

```
<Sysname> system-view
```

```
[Sysname] apn-profile test
```

```
[Sysname-apn-profile-test] authentication-mode chap user user1 password simple 123456
```

New feature: Media Stream Control (MSC) logging

This feature enables the router to generate MSC logs and send the logs to the information center.

Command reference

New command: sip log enable

Use **sip log enable** to enable Media Stream Control (MSC) logging.

Use **undo sip log enable** to disable MSC logging.

Syntax

sip log enable

undo sip log enable

Default

MSC logging is disabled.

Views

Voice view

Predefined user roles

network-admin

Usage guidelines

This command enables the router to generate MSC logs and send the logs to the information center. The information center outputs the logs to a destination according to an output rule. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

MSC logging is used for auditing purposes.

Examples

```
# Enable MSC logging.
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip log enable
```

New feature: IMSI/SN binding authentication

This feature enables the device to include the IMSI/SN information in the LCP authentication information.

Command reference

ppp lcp imsi accept

Use **ppp lcp imsi accept** to enable the client to accept the IMSI binding authentication requests from the LNS.

Use **undo ppp lcp imsi accept** to restore the default.

Syntax

ppp lcp imsi accept

undo ppp lcp imsi accept

Default

The client declines the IMSI binding authentication requests from the LNS.

Views

Interface view

Predefined user roles

network-admin

Examples

```
# Enable the client to accept the IMSI binding authentication requests from the LNS.
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi accept
```

ppp lcp imsi request

Use **ppp lcp imsi request** to enable the LNS to initiate IMSI binding authentication requests.

Use **undo ppp lcp imsi request** to restore the default.

Syntax

ppp lcp imsi request

undo ppp lcp imsi request

Default

The LNS does not initiate IMSI binding authentication requests.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable the LNS to initiate IMSI binding authentication requests.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi request
```

ppp lcp imsi string

Use **ppp lcp imsi string** *imsi-info* to configure the IMSI information on the client.

Use **undo ppp lcp imsi string** to delete the IMSI information on the client.

Syntax

ppp lcp imsi string *imsi-info*

undo ppp lcp imsi string

Default

The client automatically obtains the IMSI information from its SIM card.

Views

Interface view

Predefined user roles

network-admin

Parameters

imsi-info: Specifies the IMSI information, a case-sensitive string of 1 to 31 characters.

Examples

```
# Configure the IMSI information as imsi1.
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi string imsi1
```

ppp lcp sn accept

Use **ppp lcp sn accept** to enable the client to accept the SN binding authentication requests from the LNS.

Use **undo ppp lcp sn accept** to restore the default.

Syntax

ppp lcp sn accept

undo ppp lcp sn accept

Default

The client declines the SN binding authentication requests from the LNS.

Views

Interface view

Predefined user roles

network-admin

Examples

```
# Enable the client to accept the SN binding authentication requests from the LNS.
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp sn accept
```

ppp lcp sn request

Use **ppp lcp sn request** to enable the LNS to initiate SN binding authentication requests.

Use **undo ppp lcp sn request** to restore the default.

Syntax

ppp lcp sn request

undo ppp lcp sn request

Default

The LNS does not initiate SN binding authentication requests.

Views

Interface view

Predefined user roles

network-admin

Examples

Enable the LNS to initiate SN binding authentication requests.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi request
```

ppp lcp sn string

Use **ppp lcp sn string** *sn-info* to configure the SN information on the client.

Use **undo ppp lcp sn string** to delete the SN information on the client.

Syntax

ppp lcp sn string *sn-info*

undo ppp lcp sn string

Default

The client automatically obtains the SN information from its SIM card.

Views

Interface view

Predefined user roles

network-admin

Parameters

sn-info: Specifies the SN information, a case-sensitive string of 1 to 31 characters.

Examples

Configure the SN information as **sn1**.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp sn string sn1
```

ppp user accept-format imsi-sn split

Use **ppp user accept-format imsi-sn split** *splitchart* to configure the separator for the received authentication information.

Use **undo ppp user accept-format** to restore the default.

Syntax

ppp user accept-format imsi-sn split *splitchart*

undo ppp user accept-format

Default

No separator is configured for the received authentication information.

Views

Interface view

Predefined user roles

network-admin

Parameters

splitchart: Specifies the separator. The separator contains one character, and it can be a letter, a digit, or any sign other than the at sign (@), slash (/), and backslash (\).

Usage guidelines

By default, the authentication information contains only the client username. If you include the IMSI or SN information in the authentication information, you need to configure the separator to separate different types of information.

If no IMSI/SN information is received from the peer during the authentication process, the IMSI/SN information split from the received authentication information is used.

Examples

Configure the pound sign (#) as the separator for the authentication information.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user accept-format imsi-sn split #
```

ppp user attach-format imsi-sn split

Use **ppp user attach-format imsi-sn split *splitchart*** to configure the separator for the sent authentication information.

Use **undo ppp user attach-format** to restore the default.

Syntax

ppp user attach-format imsi-sn split *splitchart*

undo ppp user attach-format

Default

No separator is configured for the sent authentication information.

Views

Interface view

Predefined user roles

network-admin

Parameters

splitchart: Specifies the separator. The separator contains one character, and it can be a letter, a digit, or any sign other than the at sign (@), slash (/), and backslash (\).

Usage guidelines

By default, the authentication information contains only the client username. If you include the IMSI or SN information in the authentication information, you need to configure the separator to separate different types of information.

Examples

Configure the pound sign (#) as the separator for the sent authentication information.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user attach-format imsi-sn split #
```

ppp user replace

Use **ppp user replace** to replace the client username with the IMSI or SN information for authentication.

Use **undo ppp user replace** to restore the default.

Syntax

ppp user replace { imsi | sn }

undo ppp user replace

Default

The client username is used for authentication.

Views

Interface view

Predefined user roles

network-admin

Examples

Replace the client username with the IMSI information for authentication.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user replace imsi
```

New feature: Specifying a band for a 4G modem

You can specify a band for a 4G modem.

Command reference

lte band

Use **lte band** to specify a band for a 4G modem.

Use **undo lte band** to restore the default.

Syntax

lte band *band-number*

undo lte band

Default

The default setting varies by 4G modem model.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

band-number: Specifies a band for a 4G modem. The available bands vary by modem model.

Usage guidelines

This command is supported only on the following 4G modems:

- Sierra MC7354 and MC7304.
- Long Sung U8300C, U8300W, and U8300.
- WNC DM11-2.

Examples

```
# Specify band 3 for Cellular 1/0.  
<Sysname> system-view  
[Sysname] controller cellular 1/0  
[Sysname-Controller-Cellular1/0] lte band 3
```

New feature: Using tunnel interfaces as OpenFlow ports

The MSR 2600 routers support using tunnel interfaces as OpenFlow ports.

New feature: NETCONF support for ACL filtering

Support of NETCONF for ACL filtering was added.

Command reference

netconf soap http acl

Use **netconf soap http acl** to apply an ACL to NETCONF over SOAP over HTTP traffic.

Use **undo netconf soap http acl** to restore the default.

Syntax

netconf soap http acl { *acl-number* | **name** *acl-name* }

undo netconf soap http acl

Default

No ACL is applied to NETCONF over SOAP over HTTP traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**. The specified ACL must be an existing IPv4 basic ACL.

Usage guidelines

This command is not available in FIPS mode.

Only NETCONF clients permitted by the ACL can access the device through SOAP over HTTP.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only NETCONF clients in subnet 10.10.0.0/16 to access the device through SOAP over HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
```

```
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

netconf soap https acl

Use **netconf soap https acl** to apply an ACL to NETCONF over SOAP over HTTPS traffic.

Use **undo netconf soap https acl** to restore the default.

Syntax

netconf soap https acl { *acl-number* | **name** *acl-name* }

undo netconf soap https acl

Default

No ACL is applied to NETCONF over SOAP over HTTPS traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name acl-name: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**. The specified ACL must be an existing IPv4 basic ACL.

Usage guidelines

Only NETCONF clients permitted by the ACL can access the device through SOAP over HTTPS.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only NETCONF clients in subnet 10.10.0.0/16 to access the device through SOAP over HTTPS.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap https acl 2001
```

New feature: WAAS

Configuring WAAS

This release added support for the Wide Area Application Services (WAAS) feature in the DATA image on the following router series:

- MSR 800.
- MSR 2600.
- MSR 3600.
- MSR 5600.

Command reference

All commands were newly added.

For more information about the commands, see WAAS commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Support for the MKI field in SRTP or SRTCP packets

This feature enables the router to add the MKI field to outgoing SRTP or SRTCP packets. You can set the length of the MKI field.

Command reference

New command: mki

Use **mki** to add the MKI field to outgoing SRTP or SRTCP packets and set the length of the MKI field.

Use **undo mki** to restore the default.

Syntax

mki *mki-length*

undo mki

Default

Outgoing SRTP or SRTCP packets do not carry the MKI field.

Views

SIP view

Predefined user roles

network-admin

Parameters

mki-length: Specifies the length of the MKI field, in the range of 1 to 128 bytes.

Usage guidelines

This command takes effect only when SRTP is the media stream protocol for SIP calls. To specify SRTP as the medial stream protocol for SIP calls, use the **srtp** command.

Examples

Add the MKI field to outgoing SRTP or SRTCP packets and set the length of the MKI field to 1 bit.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] mki 1
```

New feature: SIP domain name

This feature enables the router to populate the CONTACT header field of outgoing SIP packets with the router's SIP domain name.

Command reference

New command: sip-domain

Use **sip-domain** to populate the CONTACT header field of outgoing SIP packets with the router's SIP domain name.

Use **undo sip-domain** to restore the default.

Syntax

sip-domain *domain-name*

undo sip-domain

Default

The router populates the CONTACT header field of an outgoing SIP packet with the IP address of the outgoing interface.

Views

SIP view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the SIP domain name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, underscore (_), hyphen (-), and dot (.).

Examples

Populate the CONTACT header field of outgoing SIP packets with the SIP domain name **abc.com**.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-domain abc.com
```

New feature: E&M logging

This feature enables the router to generate E&M logs.

Command reference

New command: em log enable

Use **em log enable** to enable E&M logging.

Use **undo em log enable** to disable E&M logging.

Syntax

em log enable

undo em log enable

Default

E&M logging is disabled.

Views

Voice view

Predefined user roles

network-admin

Usage guidelines

This command enables the router to generate E&M logs.

Examples

```
# Enable E&M logging.
<Sysname> system-view
[Sysname] voice-setup
```


[Sysname-voice] em log enable

New feature: Setting the RTC version

Setting the RTC version

The RTC protocol has the following versions: Version 3 and Version 5. Comware V3-based routers support only Version 3. Comware V5- or Comware V7-based routers support both Version 3 and Version 5.

To set the RTC version:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the RTC version.	rta rtc version { v3 v5 }	By default, the router uses Version 5.

Command reference

rta rtc version

Use **rta rtc version** to set the RTC version.

Use **undo rta rtc version** to restore the default.

Syntax

rta rtc version { v3 | v5 }

undo rta rtc version

Default

The router uses RTC Version 5.

Views

System view

Predefined user roles

network-admin

Parameters

V3: Sets the RTC version to Version 3.

V5: Sets the RTC version to Version 5.

Usage guidelines

Comware V5/V7-based routers support both RTC Version 3 and Version 5. Comware V3-based routers support only RTC Version 3.

For a Comware V5/V7-based router to communicate with a Comware V3-based, set the RTC version to Version 3 on the Comware V5/V7-based router.

For Comware V5/V7-based routers to communicate each other, set the RTC version on the routers to the same version.

Examples

```
# Set the RTC version to Version 3.
```

```
<Sysname> system-view
```

```
[Sysname] rta rtc version v3
```

New feature: Setting the maximum size of advertisement files

You can set the maximum size of advertisement files sent to wireless clients to 10 MB when the clients access the wireless network.

New feature: Support of IRF for NETCONF

Support for NETCONF was added to IRF.

New feature: Support of VCF for NETCONF

Support for NETCONF was added to VCF.

New feature: Support of SNMP for NETCONF

Support for NETCONF was added to SNMP.

New feature: Support of file system for NETCONF

Support for NETCONF was added to file system.

New feature: Support of PoE for NETCONF

Support for NETCONF was added to PoE.

New feature: Support of RMON for NETCONF

Support for NETCONF was added to RMON.

New feature: Support of policy-based routing for NETCONF

Support for NETCONF was added to policy-based routing.

New feature: Support of BGP for NETCONF

Support for NETCONF was added to BGP.

New feature: Support of OSPF for NETCONF

Support for NETCONF was added to OSPF.

New feature: Support of ping for NETCONF

Support for NETCONF was added to ping.

New feature: Support of tracer for NETCONF

Support for NETCONF was added to tracer.

New feature: Support of L2VPN for NETCONF

Support for NETCONF was added to L2VPN.

New feature: SIP support for VRF

Configuring SIP support for VRF

For information about this feature, see SIP configuration in *H3C MSR Router Series Comware 7 Voice Configuration Guide*.

Command reference

The **vpn-instance** command was added.

For information about the command, see SIP commands in *H3C MSR Router Series Comware 7 Voice Command Reference*.

New feature: IKEv2

Configuring IKEv2

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

For information about the commands, see IPsec commands in *H3C MSR Router Series Comware 7 Command Reference*.

New feature: Specifying an IKEv2 profile for an IPsec policy

Specifying an IKEv2 profile for an IPsec policy

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **ikev2-profile** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Bidirectional BFD control detection for RIP

Configuring bidirectional BFD control detection for RIP

For information about this feature, see RIP configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide*.

Command reference

The **bfd all-interfaces enable**, **rip bfd**, and **rip primary-path-detect bfd** commands were newly added.

For information about the commands, see RIP commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: OSPF router ID autoconfiguration

Automatically obtaining an OSPF router ID

For information about this feature, see OSPF configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide*.

Command reference

The **display system internal ospf event-log router-id** command was newly added and the **auto-select** keyword was added to the **ospf** command.

For information about the commands, see OSPF commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference* and OSPF probe commands in *H3C MSR Router Series Comware 7 Probe Command Reference*.

New feature: Layer 2 Ethernet link aggregation

Configuring Layer 2 aggregation groups

For information about this feature, see Ethernet link aggregation configuration in *H3C MSR Router Series Comware 7 Layer 2—LAN Switching Configuration Guide*.

Command reference

For information about the commands, see Ethernet link aggregation commands in *H3C MSR Router Series Comware 7 Layer 2—LAN Switching Command Reference*.

New feature: Setting the cable impedance for WAN interfaces

Setting the cable impedance for WAN interfaces

For information about this feature, see WAN interface configuration in *H3C MSR Router Series Comware 7 Interface Configuration Guide*.

Command reference

The **cable type** and **fe1 cable-type** commands were added.

For information about the commands, see WAN interface commands in *H3C MSR Router Series Comware 7 Interface Configuration Guide*.

New feature: Associating a static route with a track entry

Associating a static route with a track entry

For information about this feature, see static routing configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide*.

Command reference

The **track** keyword was added to the **ip route-static** command.

For information about the command, see static routing commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: VLAN tag processing rule for incoming traffic

Configuring the VLAN tag processing rule for incoming traffic

For information about this feature, see *H3C MSR Router Series Comware 7 VXLAN Configuration Guide*.

Command reference

The **l2vpn rewrite inbound tag** command was added. For information about this command, see *H3C MSR Router Series Comware 7 VXLAN Command Reference*.

New feature: IP-based portal-free rule

Configuring an IP-based portal free-rule

For information about this feature, see portal authentication configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The portal free-rule command was added.

For information about the command, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Portal redirect packet statistics

Displaying/maintaining portal redirect packet statistics

For information about this feature, see portal authentication configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **display portal redirect statistics** and **reset portal redirect statistics** commands were added.

For information about the commands, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: GDVPN

Configuring GDVPN

For information about this feature, see group domain VPN configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

For information about the commands, see group domain VPN commands in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

New feature: OpenFlow instance

Configuring the OpenFlow instance mode

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **port** keyword was added to the **classification** command.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

Binding an OpenFlow instance to ports

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **port** command was added.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

Binding an port to an OpenFlow instance

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **openflow-instance** command was added.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set

Enabling ESN for an IPsec transform set

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **esn enable** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy

Enabling TFC padding for an IPsec policy

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **tfc enable** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: SIP session refresh

Enabling SIP session refresh

In this release, you can enable SIP session refresh for a VoIP voice entity.

Command reference

New command: voice-class sip session refresh

Use **voice-class sip session refresh** to enable SIP session refresh for a VoIP entity.

Use **undo voice-class sip session refresh** to disable SIP session refresh for a VoIP entity.

Syntax

voice-class sip session refresh [global]

undo voice-class sip session refresh

Default

A VoIP entity uses the global configuration for SIP session refresh.

Views

VoIP entity view

Predefined user roles

network-admin

Parameters

global: Applies the global configuration for SIP session refresh to the VoIP entity.

Usage guidelines

The configuration for SIP session refresh in VoIP entity view takes priority over that in SIP view.

Examples

Enable SIP session refresh for VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip session refresh
```

Apply the global configuration for SIP session refresh to VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip session refresh global
```

Modified feature: License restrictions for POS terminal access

Feature change description

You can install licenses to increase the concurrent transaction threshold for each TCP connection supported by the device. If the device does not support the licenses, or no licenses are installed, the threshold varies by device model.

Modified feature: Displaying and maintaining Frame Relay

Feature change description

The **-info** part was removed from the syntax of the following commands:

- **display fr inarp-info.**
- **display fr lmi-info.**
- **display fr map-info.**
- **display fr pvc-info.**

Command changes

Modified command: display fr inarp-info

Old syntax

display fr inarp-info [**interface** *interface-type interface-number*]

New syntax

display fr inarp [**interface** *interface-type interface-number*]

Views

Any view

Command change description

The command syntax was changed from **display fr inarp-info** to **display fr inarp**.

Modified command: display fr lmi-info

Old syntax

display fr lmi-info [**interface** *interface-type interface-number*]

New syntax

display fr lmi [**interface** *interface-type interface-number*]

Views

Any view

Command change description

The command syntax was changed from **display fr lmi-info** to **display fr lmi**.

Modified command: display fr map-info

Old syntax

display fr map-info [**interface** *interface-type interface-number*]

New syntax

display fr map [**interface** *interface-type interface-number*]

Views

Any view

Command change description

The command syntax was changed from **display fr map-info** to **display fr map**.

Modified command: display fr pvc-info

Old syntax

display fr pvc-info [**interface** *interface-type interface-number*] [**dlci** *dlci-number*]

New syntax

display fr pvc [**interface** *interface-type interface-number*] [**dlci** *dlci-number*]

Views

Any view

Command change description

The command syntax was changed from **display fr pvc-info** to **display fr pvc**.

Modified feature: Displaying track entry information

Feature change description

The following fields were added to the output of the **display track** command:

- IP route.
- VPN instance name.
- Protocol.
- Nexthop interface.

Command changes

Modified command: display track

Syntax

```
display track { track-entry-number | all }
```

Views

Any view

Change description

The following fields were added to the command output:

- IP route.
- VPN instance name.
- Protocol.
- Nexthop interface.

Modified feature: User profile

Feature change description

This release added support for QoS policy configuration in user profile view.

Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes

Feature change description

This release added support for the IPsec tunnel mode and VXLAN tunnel mode on a tunnel interface.

Command changes

Modified command: interface tunnel

Old syntax

```
interface tunnel number [ mode { advpn { gre | udp } [ ipv6 ] | ds-lite-aftr | evi | gre [ ipv6 ] |  
ipv4-ipv4 | ipv6 | ipv6-ipv4 [ 6to4 | auto-tunnel | isatap ] | mpls-te | nve } ]
```

New syntax

```
interface tunnel number [ mode { advpn { gre | udp } [ ipv6 ] | ds-lite-afr | evi | gre [ ipv6 ] | ipsec  
[ ipv6 ] | ipv4-ipv4 | ipv6 | ipv6-ipv4 [ 6to4 | auto-tunnel | isatap ] | mpls-te | nve | vxlan } ]
```

Views

System view

Change description

The following parameters were added to the command:

- **mode ipsec**: Specifies the IPv4 IPsec tunnel mode.
- **mode ipsec ipv6**: Specifies the IPv6 IPsec tunnel mode.
- **mode vxlan**: Specifies the VXLAN tunnel mode.

Modified feature: PKI certificate auto-renewal

Feature change description

Support for certificate auto-renewal was added to PKI.

Command changes

Modified command: certificate request mode

Old syntax

```
certificate request mode { auto [ password { cipher | simple } string ] | manual }
```

New syntax

```
certificate request mode { auto [ password { cipher | simple } string | renew-before-expire days  
[ reuse-public-key ] [ auto-append common-name ] ] * | manual }
```

Views

PKI domain view

Change description

The following keywords were added to the command:

- **renew-before-expire *days***: Configures the system to automatically request a new certificate the specified number of days before the current certificate expires. The value range for the *days* argument is 0 to 365. Value 0 indicates that the request for a new certificate is made when the old certificate expires, which might cause service interruptions.

- **reuse-public-key:** Reuses the key pair in the old certificate for the new certificate. If you do not specify this keyword, the system generates a new key pair for the new certificate. The old key pair is replaced with the new one when the new certificate is received from the CA.
- **auto-append common-name:** Automatically appends random data to the common name of the PKI entity for the new certificate. If you do not specify this keyword, the common name of the PKI entity will be unchanged in the new certificate.

New command: display pki certificate renew-status

Use **display pki certificate renew-status** to display the certificate renewal status for a PKI domain.

Syntax

display pki certificate renew-status [**domain** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in Table 3. If you do not specify a domain name, this command displays the certificate renewal status for all PKI domains.

Table 5 Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar		Quotation marks	"
Colon	:	Apostrophe	'

Examples

Display the certificate renewal status for all PKI domains.

```
<Sysname> display pki certificate renew-status
```

```
Domain name: domain1
```

```
Renew time: 03:12:05 2015/12/07
```

```
Renew public key:
```

```
Key type: RSA
```

```
Time when key pair created: 15:40:48 2015/05/12
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
```

```
667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
2DA4C04EF5AE0835090203010001
```

The command output indicates that the **reuse-public-key** keyword was not configured for PKI domain **domain1** and a new key pair was created for the new certificate.

Display the certificate renewal status for PKI domain **domain1**.

```
<Sysname> display pki certificate renew-status domain1
Domain name: domain1
Renew time: 03:12:05 2013/12/07
Renew public key:
Key type: RSA
Time when key pair created: 15:40:48 2013/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
2DA4C04EF5AE0835090203010001
```

Table 6 Command output

Field	Description
Renew time	Time when a new certificate will be requested.
Renew public key	Information about the new key pair created for the certificate.
Key type	Key pair type, which can be RSA, DSA, or ECDSA.
Time when key pair created	Time when the key pair was created.
Key code	Public key data.

Modified feature: Configuring the PKI entity DN

Feature change description

Support for the **subject-dn** command was added to PKI. You can use the command to configure the full subject DN string. Each attribute can be specified multiple times with different values.

Command changes

New command: subject-dn

Use **subject-dn** to configure the DN for a PKI entity.

Use **undo subject-dn** to restore the default.

Syntax

subject-dn *dn-string*

undo subject-dn

Default

No DN is configured for a PKI entity.

Views

PKI entity view

Default command level

network-admin

Parameters

dn-string: Specifies the DN for the PKI entity, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The subject DN string is a sequence of *attribute=value* pairs separated by commas. Each attribute can be specified multiple times with different values. Supported DN attributes are:

- **CN**—Common-name.
- **C**—Country code.
- **L**—Locality.
- **O**—Organization.
- **OU**—Organization unit.
- **ST**—State or province.

After this command is configured, the following commands do not take effect:

- **common-name**
- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

If you configure this command multiple times, the most recent configuration takes effect.

Examples

```
# Configure the DN for PKI entity en.  
<Sysname> system-view  
[Sysname] pki entity en  
[Sysname-pki-entity-en] subject-dn  
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

Modified feature: ADVPN

Feature change description

In this release, you can configure ADVPN group names and ADVPN group-to-QoS policy mappings.

Command changes

New command: advpn group

Use **advpn group** to configure an ADVPN group name.

Use **undo advpn group** to restore the default.

Syntax

advpn group *group-name*

undo advpn group

Default

No ADVPN group name is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

Usage guidelines

This command must be configured on the tunnel interface of a spoke. The spoke sends the ADVPN group name in a hub-spoke tunnel establishment request to a hub. The hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel. If no match is found, the hub does not apply a QoS policy to the hub-spoke tunnel.

If you modify the ADVPN group name after the tunnel is established, the spoke will inform the hub of the modification. The hub will look for an ADVPN group-to-QoS policy mapping that matches the new ADVPN group name and apply the QoS policy in the new mapping.

As a best practice, do not configure an ADVPN group name and apply a QoS policy on the same tunnel interface.

Examples

Configure **aaa** as the ADVPN group name.

```
<Sysname> system-view
[Sysname] interface tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn group aaa
```

New command: advpn map group

Use **advpn map group** to configure a mapping between an ADVPN group and a QoS policy.

Use **undo advpn map group** to delete a mapping between an ADVPN group and a QoS policy.

Syntax

advpn map group *group-name* **qos-policy** *policy-name* **outbound**

undo advpn map group *group-name*

Default

No ADVPN group-to-QoS policy mappings are configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

qos-policy *policy-name*: Specifies the QoS policy name, a case-sensitive string of 1 to 31 characters.

outbound: Applies the QoS policy to the outbound direction.

Usage guidelines

This command must be configured on the tunnel interface of a hub. After receiving a hub-spoke tunnel establishment request from a spoke, the hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name carried in the request. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel.

You can configure multiple ADVPN group-to-QoS policy mappings on a tunnel interface.

You can map multiple ADVPN groups to a QoS policy. You can map an ADVPN group to only one QoS policy.

As a best practice, do not configure an ADVPN group-to-QoS policy mapping and apply a QoS policy on the same tunnel interface.

Examples

Configure a mapping between ADVPN group **aaa** and QoS policy **bbb** on **Tunnel1**.

```
<Sysname> system-view
[Sysname] interface Tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn map group aaa qos-policy bbb outbound
```

Modified feature: Telnet redirect

Feature change description

In this release, a Telnet redirect user is authenticated by using the authentication settings for the TTY line. The device displays only Telnet redirect authentication information and the authentication result. It does not display the copyright statement.

Support for Telnet redirect authentication was removed from MSR56 routers.

Modified feature: DHCP snooping performance optimization

Feature change description

On a Layer 3 physical interface without subinterface, link aggregation, or snooping configured, the **dhcp snooping enable** command was optimized to cause only a slight impact on receiving non-DHCP packets. If you configure other services on the interface, the performance varies with the services you configure.

Modified feature: OSPF performance optimization

Feature change description

You can set a fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

The value range for the LSU packet sending interval was changed to 0 to 1000 milliseconds.

Command changes

Modified command: spf-schedule-interval

Old syntax

spf-schedule-interval { *maximum-interval* [*minimum-interval* [*incremental-interval*]] }

New syntax

spf-schedule-interval { *maximum-interval* [*minimum-interval* [*incremental-interval*]] | *millisecond interval* }

Views

OSPF view

Change description

The *millisecond interval* argument was added to the command. You can specify this argument to set a fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

Modified command: transmit-pacing

Syntax

transmit-pacing interval *interval* **count** *count*

Views

OSPF view

Change description

Before modification: The value range for the *interval* argument was 10 to 1000 milliseconds.

After modification: The value range for the *interval* argument is 0 to 1000 milliseconds.

Modified feature: POS terminal access

Feature change description

The **posa auto-stop-service enable** command added the function of setting the access interfaces for all E1POS terminal templates to reply with busy tones when all FEPs are unreachable.

Command changes

Modified command: `posa auto-stop-service enable`

Syntax

`posa auto-stop-service enable`

Views

System view

Change description

Before modification, this command enables automatic shutdown of the listening ports for TCP-based POS terminal templates when all FEPs that correspond to TCP-based POS application templates are unreachable. When any of the FEPs becomes reachable, the router automatically opens the listening ports for all TCP-based POS terminal templates.

After modification, this command enables the router to automatically perform the following operations when all FEPs that correspond to TCP-based POS application templates are unreachable:

- Shuts down the listening ports for all TCP-based POS terminal templates.
- Sets the access interfaces for all E1POS terminal templates to reply with busy tones.

When any of the FEPs becomes reachable, the router automatically performs the following operations:

- Opens the listening ports for all TCP-based POS terminal templates.
- Disables busy tone for all E1POS terminal templates.

Modified feature: License

Feature change description

The device uses high encryption algorithms by default and does not require a license.

Modified feature: IP performance optimization

Feature change description

The device supports recording MAC addresses in TCP packets. You can also configure the device to record the MAC address of the local device in TCP packets.

Command changes

New command: tcp mac-record enable

Use **tcp mac-record enable** to enable MAC address recording in TCP packets.

Use **undo tcp mac-record enable** to disable MAC address recording in TCP packets.

Syntax

tcp mac-record enable

undo tcp mac-record enable

Default

MAC address recording in TCP packets is disabled.

Views

Interface view

Default command level

network-admin

Usage guidelines

This feature records the MAC address of the packet originator in a TCP option. When an attack occurs, the administrator can quickly locate the attack source according to the recorded MAC addresses.

Examples

```
# Enable MAC address recording in TCP packets on GigabitEthernet 1/0/1.
```

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 0/1
```

```
[Sysname-GigabitEthernet0/1] tcp mac-record enable
```

New command: tcp mac-record local

Use **tcp mac-record local** to record the MAC address of the local device in TCP packets.

Use **undo tcp mac-record local** to restore the default.

Syntax

tcp mac-record local *mac-address*

undo tcp mac-record local

Default

The destination MAC address is recorded.

Views

System view

Default command level

network-admin

Parameters

mac-address: Specifies the MAC address of the local device. The MAC address cannot be all 0s, broadcast MAC address, or multicast MAC address.

Usage guidelines

To make this command take effect, you must enable MAC address recording in TCP packets by using the **tcp mac-record enable** command.

Examples

```
# Record the MAC address of the local device 0605-0403-0201 in TCP packets.
```

```
<Sysname> system-view
```

```
[Sysname] tcp mac-record local 0605-0403-0201
```

Modified feature: AAA

Feature change description

Starting from this software version, you can configure the authorization method for IKE extended authentication.

Command changes

New command: authorization ike

Use **authorization ike** to configure the authorization method for IKE extended authentication.

Use **undo authorization ike** to restore the default.

Syntax

In non-FIPS mode:

```
authorization ike { local [ none ] | none | radius-scheme radius-scheme-name [ local ] [ none ] }
```

```
undo authorization ike
```

In FIPS mode:

```
authorization ike { local | radius-scheme radius-scheme-name [ local ] }
```

```
undo authorization ike
```

Default

The default authorization method for the ISP domain is used for IKE extended authentication.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

In ISP domain **test**, perform local authorization for IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ike local
```

In ISP domain **test**, use RADIUS scheme **rd** as the primary authorization method and local authorization as the backup authorization method for IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ike radius-scheme rd local
```

Modified feature: Configuring a cellular interface for a 3G/4G modem

Feature change description

In this release, you can set the RSSI thresholds for a 3G/4G modem.

Command changes

New command: rssi

Use **rssi** to set the RSSI thresholds for a 3G/4G modem.

Use **undo rssi** to restore the default.

Syntax

```
rsi { 1xrtt | evdo | gsm | lte } { low lowthreshold | medium mediumthreshold } *  
undo rsi { 1xrtt | evdo | gsm | lte } [ low | medium ]
```

Default

The lower and upper thresholds for a 3G/4G modem are –150 dBm and 0 dBm, respectively.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

1xrtt: Specifies the 1xRTT mode.

evdo: Specifies the EVDO mode.

gsm: Specifies the GSM mode.

lte: Specifies the LTE mode.

low *lowthreshold*: Specifies the lower RSSI threshold value in the range of 0 to 150, which represent a lower RSSI threshold in the range of –150 dBm to 0 dBm. The value of *lowthreshold* cannot be smaller than the value of *mediumthreshold* because the system automatically adds a negative sign to the RSSI thresholds.

medium *mediumthreshold*: Specifies the upper RSSI threshold value in the range of 0 to 150, which represent an upper RSSI threshold in the range of –150 dBm to 0 dBm.

Usage guidelines

The device performs the following operations based on the actual RSSI of the 3G/4G modem:

- Sends a trap that indicates high RSSI when the RSSI exceeds the upper threshold.
- Sends a trap that indicates normal RSSI when the RSSI is between the lower threshold and upper threshold (included).
- Sends a trap that indicates low RSSI when the RSSI drops to or below the lower threshold.
- Sends a trap that indicates low RSSI every 10 minutes when the RSSI remains equal to or smaller than the lower threshold.

To view the RSSI change information for a 3G/4G modem, use the **display cellular** command.

Examples

```
# Set the lower threshold for a 3G/4G modem in GSM mode to –110 dBm.
```

```
<Sysname> system-view  
[Sysname] interface cellular 0/0  
[Sysname-Cellular0/0] rsi gsm low 110
```

Modified feature: QoS on VXLAN tunnel interfaces

Feature change description

This software version added support for QoS in the outbound direction of VXLAN tunnel interfaces.

Command changes

None.

Modified feature: Option 60 encapsulation in DHCP replies

Feature change description

Disabling Option 60 encapsulation in DHCP replies.

Modified feature: MPLS QoS support for matching the EXP field

Feature change description

In this release, MPLS QoS supports matching the EXP fields in both the topmost (first) MPLS label and the second MPLS label.

Command changes

New command: `if-match second-mpls-exp`

Use **`if-match second-mpls-exp`** to define a criterion to match the EXP field in the second MPLS label.

Use **`undo if-match second-mpls-exp`** to delete the match criterion.

Syntax

if-match [**not**] **second-mpls-exp** *exp-value*&<1-8>

undo if-match [**not**] **second-mpls-exp** *exp-value*&<1-8>

Default

No criterion is defined to match the EXP field in the second MPLS label.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

not: Matches packets not conforming to the specified criterion.

exp-value&<1-8>: Specifies a space-separated list of up to eight EXP values. The value range for the *exp-value* argument is 0 to 7. If the same MPLS EXP value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.

Examples

```
# Define a criterion to match packets with EXP value 3 or 4 in the second MPLS label.  
<Sysname> system-view  
[Sysname] traffic classifier database  
[Sysname-classifier-database] if-match second-mpls-exp 3 4
```

Modified feature: MPLS QoS support for marking the EXP field

Feature change description

In this release, MPLS QoS supports marking the EXP fields in both the topmost (first) MPLS label and the second MPLS label.

Command changes

New command: remark second-mpls-exp

Use **remark second-mpls-exp** to configure an EXP value marking action for the second MPLS label in a traffic behavior.

Use **undo remark second-mpls-exp** to delete the action.

Syntax

remark second-mpls-exp *second-mpls-exp-value*

undo remark second-mpls-exp *second-mpls-exp-value*

Default

No EXP value marking action for the second MPLS label is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

second-mpls-exp-value: Specifies an EXP value for the second MPLS label, in the range of 0 to 7.

Examples

Define a traffic behavior to mark packets with EXP value 3 for the second MPLS label.

```
<Sysname> system-view
```

```
[Sysname] traffic behavior b1
```

```
[Sysname-behavior-b1] remark second-mpls-exp 3
```

Modified feature: Automatic configuration

Feature change description

A limit was added to the number of automatic attempts. After the limit is reached, the automatic configuration process ends.

If you set the limit to 0, only one automatic configuration attempt is allowed.

Modified feature: User profile

Feature change description

In this release, the user profile name supports using dots (.).

Command change

Modified command: user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

Views

System view

Change description

Before modification: The user profile name is a case-sensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_), and the name must start with an English letter.

After modification: The user profile name is a case-sensitive string of 1 to 31 characters. Valid characters are letters, digits, underscores (_), and dots (.), and the name must start with an English letter.

Modified feature: Default size of the TCP receive and send buffer

Feature change description

The default value for the TCP receive and send buffer size was changed to 63 KB.

Command changes

Modified command: tcp window

Syntax

tcp window *window-size*

undo tcp window

Views

System view

Change description

Before modification: The default value for the *window-size* argument was 64 KB.

After modification: The default value for the *window-size* argument is 63 KB.

Modified feature: Obtaining fan and power module vendor information

Feature change description

Support was added for you to obtain fan and power module vendor information through MIB.

Modified feature: Support for per-packet load sharing

Feature change description

The **per-packet** keyword was added to the **ip load-sharing mode** command to support per-packet load sharing.

Command changes

Modified command: ip load-sharing mode

Old syntax

Centralized devices:

```
ip load-sharing mode per-flow [ dest-ip | dest-port | ip-pro | src-ip | src-port ] * ]
```

Centralized IRF devices—Distributed devices—In standalone mode:

```
ip load-sharing mode per-flow [ dest-ip | dest-port | ip-pro | src-ip | src-port ] * ] [ slot slot-number ]
```

Distributed devices—In IRF mode:

```
ip load-sharing mode per-flow [ dest-ip | dest-port | ip-pro | src-ip | src-port ] * ] [ chassis chassis-number slot slot-number ]
```

New syntax

Centralized devices:

```
ip load-sharing mode { per-flow [ [ dest-ip | dest-port | ip-pro | src-ip | src-port ] * ] | per-packet }
```

Centralized IRF devices—Distributed devices—In standalone mode:

```
ip load-sharing mode { per-flow [ dest-ip | dest-port | ip-pro | src-ip | src-port ] * ] | per-packet }
```

Distributed devices—In IRF mode:

```
ip load-sharing mode { per-flow [ dest-ip | dest-port | ip-pro | src-ip | src-port ] * ] | per-packet }
```

Views

System view

Change description

The **per-packet** keyword was added to the **ip load-sharing mode** command to support per-packet load sharing.

Modified feature: Default user role

Feature change description

The default user role can be changed. The *role-name* argument was added to the **role default-role enable** command for specifying a user role as the default user role.

Command changes

Modified command: role default-role enable

Old syntax

```
role default-role enable
```

```
undo role default-role enable
```

New syntax

```
role default-role enable [ role-name ]
```

```
undo role default-role enable
```

Views

System view

Change description

Before modification: The default user role is network-operator.

After modification: The *role-name* argument was added to specify any user role that exists in the system as the default user role. The argument is a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the default user role is network-operator.

Modified feature: Debugging

Feature change description

The **all** keyword and the **timeout** *time* option were removed from the **debugging** command. You can no longer use the **debugging all** command to enable debugging for all modules or specify the timeout time for the **debugging all** command.

Command changes

Modified command: debugging

Old syntax

```
debugging { all [ timeout time ] | module-name [ option ] }
```

```
undo debugging { all | module-name [ option ] }
```

New syntax

```
debugging module-name [ option ]
```

```
undo debugging module-name [ option ]
```

Views

User view

Change description

The following parameters were removed from the **debugging** command:

- **all**: Enables debugging for all modules.

timeout *time*: Specifies the timeout time for the **debugging all** command. The system automatically executes the **undo debugging all** command after the timeout time. The *time* argument is in the range of 1 to 1440 minutes. If you do not specify a timeout time, you must manually execute the **undo debugging all** command to disable debugging for all modules.

Modified feature: SSH username

Feature change description

In this release, an SSH username cannot be **a**, **al**, **all**, or include the following characters:
\\ / : * ? < >

The at sign (@) can only be used in the username format *pureusername@domain* when the username contains an ISP domain name.

Command changes

Modified command: ssh user

Syntax

In non-FIPS mode:

```
ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type  
{ password | { any | password-publickey | publickey } assign { pki-domain domain-name |  
publickey keyname } }
```

```
undo ssh user username
```

In FIPS mode:

```
ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type  
{ password | password-publickey assign { pki-domain domain-name | publickey keyname } }
```

```
undo ssh user username
```

Views

System view

Change description

Before modification: The *username* argument is a case-insensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the format *pureusername@domain*.

After modification: The *username* argument is a case-insensitive string of 1 to 80 characters, excluding **a**, **al**, **all**, and the following characters:
\\ / : * ? < >

The at sign (@) can only be used in the username format *pureusername@domain* when the username contains an ISP domain name. The pure username can contain 1 to 55 characters and the domain name can contain 1 to 24 characters. The whole username cannot exceed 80 characters.

Modified feature: IS-IS hello packet sending interval

Feature change description

The value range of the interval for sending hello packets was changed to 1 to 255 seconds.

Command changes

Modified command: isis timer hello

Syntax

```
isis timer hello seconds [ level-1 | level-2 ]
```

```
undo isis timer hello [ level-1 | level-2 ]
```

Views

Interface view

Change description

The value range for the *seconds* argument was changed to 1 to 255 seconds.

Modified feature: MP-group interface numbering

In this release, the numbering for MP-group interfaces is changed.

Modified feature: Setting the global link-aggregation load-sharing mode

Feature change description

The **bandwidth-usage** keyword was added to the **link-aggregation global load-sharing mode** command. You can set the global load sharing mode to load share traffic based on bandwidth usage.

Command changes

Modified command: link-aggregation global load-sharing mode

Old syntax

```
link-aggregation global load-sharing mode { destination-ip | destination-mac |  
destination-port | mpls-label1 | source-ip | source-mac | source-port } *
```

```
undo link-aggregation global load-sharing mode
```

New syntax

```
link-aggregation global load-sharing mode { bandwidth-usage | destination-ip |  
destination-mac | destination-port | mpls-label1 | source-ip | source-mac | source-port } *  
  
undo link-aggregation global load-sharing mode
```

Views

System view

Change description

The **bandwidth-usage** keyword was added. You can specify this keyword to set the global load sharing mode to load share traffic based on bandwidth usage.

Modified feature: 802.1X redirect URL

Feature change description

The value range for the *url-string* argument was changed to 1 to 256 characters for the **dot1x ead-assistant url** command.

Command changes

Modified command: dot1x ead-assistant url

Syntax

```
dot1x ead-assistant url url-string
```

Views

System view

Change description

Before modification: The value range for the *url-string* argument is 1 to 64 characters.

After modification: The value range for the *url-string* argument is 1 to 256 characters.

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Feature change description

You can specify a source interface for tracing NTP servers from the reference source to the primary NTP server.

Command changes

Modified command: display ntp-service trace

Old syntax

```
display ntp-service trace
```

New syntax

```
display ntp-service trace [ source interface-type interface-number ]
```

Views

Any view

Change description

The **source** *interface-type interface-number* option was added to the **display ntp-service trace** command.

Modified feature: Saving, rolling back, and loading the configuration

The following configuration guidelines were added when you use NETCONF to save, roll back, or load the configuration:

- The save, rollback, and load operations supplement NETCONF requests. Performing the operations might consume a lot of system resources.
- Do not perform the save, rollback, or load operation when another user is performing the operation. If multiple users simultaneously perform the save, rollback, or load operation, the result returned to each user might be inconsistent with the user request.

Modified feature: Displaying information about SSH users

Feature change description

In this release, the **display ssh user-information** command does not display the public key name for an SSH user that uses password authentication.

Command changes

Modified command: display ssh user-information

Syntax

```
display ssh user-information [ username ]
```

Views

Any view

Change description

Before modification: The **User-public-key-name** field in the command output displays **null** for an SSH user that uses password authentication.

After modification: The **User-public-key-name** field in the command output is blank for an SSH user that uses password authentication.

Modified feature: SIP trusted nodes

Configuring SIP trusted nodes

In this release, you can enable the trusted node feature by using the **ip address trusted authenticate** command. You also can display information about SIP trusted nodes by using the **display voice ip address trusted list** command.

Command changes

The **display voice ip address trusted list** and **ip address trusted authenticate** commands were added.

New command: display voice ip address trusted list

Use **display voice ip address trusted list** to display information about trusted nodes.

Syntax

display voice ip address trusted list

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays trusted nodes in the trusted node list and call destination IP addresses.

Examples

Display information about trusted nodes.

```
<Sysname> display voice ip address trusted list
IP address trusted authentication: Enabled
```

VoIP entity IP addresses:

Entity tag	State	SIP IP address
-----	----	-----
20	Up	192.168.4.110
53232	Down	192.168.4.210
55555	Up	192.168.4.210
9613	Up	192.168.4.125

IP address trusted list:

```
192.168.4.0 255.255.255.0
192.168.5.120 255.255.255.255
```

Table 7 Command output

Field	Description
IP address trusted authentication	Whether IP address trusted authentication is enabled: • Enabled. • Disabled.
VoIP entity IP addresses	Trusted IP addresses for VoIP entities.
Entity tag	Tag of a VoIP entity.
State	Status of a VoIP entity: • Up. • Down.
SIP IP address	Call destination IP address of a VoIP entity.
IP address trusted list	List of trusted nodes.

New command: ip address trusted authenticate

Use **ip address trusted authenticate** to enable IP address trusted authentication.

Use **undo ip address trusted authenticate** to disable IP address trusted authentication.

Syntax

ip address trusted authenticate

undo ip address trusted authenticate

Default

IP address trusted authentication is disabled. All nodes are regarded as trusted, and the device accepts calls from any nodes.

Views

SIP view

Predefined user roles

network-admin

Usage guidelines

After you enable this feature, the device accepts calls only from trusted nodes.

For calls to be successfully established, configure the proxy server, registrars, the DNS server, and the MWI server as trusted nodes.

Examples

```
# Enable IP address trusted authentication.
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] ip address trusted authenticate
```

Modified feature: IPsec ESP encryption algorithms

Feature change description

Support for the following IPsec ESP encryption algorithms was added in high encryption mode:

- AES algorithm in CTR mode.
- Camellia algorithm in CBC mode.
- GMAC algorithm.
- GCM algorithm.

- SM1 algorithm in CBC mode.
- SM4 algorithm.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following arguments were added to the **esp encryption-algorithm** command:

- *aes-ctr-128*.
- *aes-ctr-192*.
- *aes-ctr-256*.
- *camellia-cbc-128*.
- *camellia-cbc-192*.
- *camellia-cbc-256*.
- *gmac-128*.
- *gmac-192*.
- *gmac-256*.
- *gcm-128*.
- *gcm-192*.
- *gcm-256*.
- *sm1-cbc-128*.
- *sm1-cbc-192*.
- *sm1-cbc-256*.
- *sm4-cbc*.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

Modified feature: IPsec ESP authentication algorithms

Feature change description

Support for the following IPsec ESP authentication algorithms was added:

- AES-XCBC-MAC.
- HMAC-SHA-25.

- HMAC-SHA-384.
- HMAC-SHA-512.
- HMAC-SM3.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following arguments were added to the **esp authentication-algorithm** command:

- *aes-xcbc-mac*.
- *sha256*.
- *sha384*.
- *sha512*.
- *sm3*.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

Modified feature: IPsec AH authentication algorithms

Feature change description

Support for the following IPsec AH authentication algorithms was added:

- AES-XCBC-MAC.
- HMAC-SHA-256.
- HMAC-SHA-384.
- HMAC-SHA-512.
- HMAC-SM3.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following arguments were added to the **ah authentication-algorithm** command:

- *aes-xcbc-mac*.

- *sha256.*
- *sha384.*
- *sha512.*
- *sm3.*

For more information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

Modified feature: Specifying an encryption algorithm for an IKE proposal

Feature change description

In this release, you can specify the following encryption algorithms for an IKE proposal:

- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following keywords were added to the **encryption-algorithm** command:

- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

Modified feature: Specifying an authentication algorithm for an IKE proposal

Feature change description

In this release, you can specify the *sm3* authentication algorithm for an IKE proposal.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The *sm3* argument was added to the **authentication-algorithm** command.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

Modified feature: Generating asymmetric key pairs

Feature change description

In this release, you can generate ECDSA key pairs by using the *secp384r1* elliptic curve.

For information about this feature, see public key management in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The **secp384r1** keyword was added to the **public-key local create** command.

For information about the command, see public key management commands in *H3C MSR Router Series Comware 7 Command Reference*.

Modified feature: Specifying an ECDSA key pair for certificate request

Feature change description

In this release, you can specify an ECDSA key pair with a specific key length for certificate request. Supported key lengths are:

- 192 bits.
- 256 bits.
- 384 bits.

For information about this feature, see PKI in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following keywords were added to the **public-key ecdsa name** command:

- **secp192r1**.
- **secp256r1**.
- **secp384r1**.

For information about the command, see PKI commands in *H3C MSR Router Series Comware 7 Command Reference*.

Modified feature: Setting the electrical impedance

Feature change description

In this release, the electrical impedance value of South Africa was added to the **impedance** command.

For information about this feature, see voice interface configuration in *H3C MSR Router Series Comware 7 Voice Configuration Guide*.

Command changes

The value south-africa was added to the *country-name* argument of the **impedance** command.

For information about the command, see voice interface commands in *H3C MSR Router Series Comware 7 Voice Command Reference*.

Modified feature: POS access statistics, SNMP notifications for POS access, and NII

Feature change description

Enabling SNMP notifications for POS access

For information about this feature, see POS terminal access in *H3C MSR Router Series Comware 7 Terminal Access Configuration Guide*.

Configuring the alarm threshold for the low NII transaction success rate

For information about this feature, see POS terminal access in *H3C MSR Router Series Comware 7 Terminal Access Configuration Guide*.

POS terminal packet statistics based on E1POS interfaces

For information about this feature, see POS terminal access in *H3C MSR Router Series Comware 7 Terminal Access Configuration Guide*.

Displaying and maintaining terminal access

For information about this feature, see POS terminal access in *H3C MSR Router Series Comware 7 Terminal Access Configuration Guide*.

Command changes

Modified command: snmp-agent trap enable posa

The **e1-dial-falling**, **fcm-trade-abnomal**, and **trade-success-falling** keywords were added.

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New command: trade-exchanges

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New command: posa trade-falling-threshold

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New command: posa e1-dial-falling-threshold

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New command: display posa statistics caller-id

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New command: display posa statistics caller-ip

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

New command: display posa statistics nii

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

Modified command: reset posa statistics

The **nii** [*nii-id*] option was added.

For information about the command, see POS terminal access commands in *H3C MSR Router Series Comware 7 Terminal Access Command Reference*.

Modified feature: QoS MIB

Feature change description

In this release, QoS MIB information changed.

Modified feature: Enabling PFS for an IPsec transform set

Feature change description

In this release, you can enable PFS using 256-bit or 384-bit ECP Diffie-Hellman group for an IPsec transform set.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The **dh-group19** and **dh-group20** keywords were added to the **pfs** command.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

Removed feature: Tiny proxy

Feature change description

The tiny proxy feature was removed.

Removed command

http-proxy

Syntax

http-proxy

undo http-proxy

Views

System view

Removed feature: Displaying switching fabric channel usage

Feature change description

Support for displaying switching fabric channel usage on interface cards was removed.

Removed command

display fabric utilization

Syntax

In standalone mode:

display fabric utilization [**slot** *slot-number*]

In IRF mode:

display fabric utilization [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Release 0304

This release has the following changes:

New feature: [Setting the RTC version](#)

New feature: [Setting the maximum size of advertisement files](#)

New feature: [IRF](#)

New feature: [Frame Relay](#)

New feature: [EVI](#)

New feature: [VPLS](#)

New feature: [Multicast VPN support for inter-AS option B](#)

Modified feature: [802.1X redirect URL](#)

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Modified feature: Saving, rolling back, and loading the configuration

Modified feature: Displaying information about SSH users

Removed feature: Displaying fabric utilization

New feature: Setting the RTC version

Configuring Setting the RTC version

The RTC protocol has the following versions: Version 3 and Version 5. Comware V3-based routers support only Version 3. Comware V5- or Comware V7-based routers support both Version 3 and Version 5.

To set the RTC version:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the RTC version.	rta rtc version { v3 v5 }	By default, the router uses Version 5.

Command reference

rta rtc version

Use **rta rtc version** to set the RTC version.

Use **undo rta rtc version** to restore the default.

Syntax

rta rtc version { v3 | v5 }

undo rta rtc version

Default

The router uses RTC Version 5.

Views

System view

Predefined user roles

network-admin

Parameters

V3: Sets the RTC version to Version 3.

V5: Sets the RTC version to Version 5.

Usage guidelines

Comware V5/V7-based routers support both RTC Version 3 and Version 5. Comware V3-based routers support only RTC Version 3.

For a Comware V5/V7-based router to communicate with a Comware V3-based, set the RTC version to Version 3 on the Comware V5/V7-based router.

For Comware V5/V7-based routers to communicate each other, set the RTC version on the routers to the same version.

Examples

```
# Set the RTC version to Version 3.
```

```
<Sysname> system-view
```

```
[Sysname] rta rtc version v3
```

New feature: Setting the maximum size of advertisement files

Configuring the maximum size of advertisement files

You can set the maximum size of advertisement files sent to wireless clients to 10 MB when the clients access the wireless network.

Command reference

None

New feature: IRF

Configuring IRF

See *HP MSR Router Series Virtual Technologies Configuration Guide (V7)*.

Command reference

See *HPE FlexNetwork MSR Router Virtual Technologies Command Reference(V7)*.

New feature: Frame Relay

Configuring Frame Relay

See *HPE FlexNetwork MSR Routers Layer 2 - WAN Configuration Guide(V7)*.

Command reference

See *HPE FlexNetwork MSR Routers Layer 2 - WAN Command Reference(V7)*.

New feature: EVI

Configuring EVI

See *HPE FlexNetwork MSR Router EVI Configuration Guide (V7)*.

Command reference

See *HPE FlexNetwork MSR Router EVI Command Reference(V7)*.

New feature: VPLS

Configuring VPLS

See *HPE FlexNetwork MSR Routers MPLS Configuration Guide(V7)*.

Command reference

See *HPE FlexNetwork MSR Routers MPLS Command Reference(V7)*.

New feature: Multicast VPN support for inter-AS option B

Configuring Multicast VPN support for inter-AS option B

See *HPE FlexNetwork MSR Routers IP Multicast Configuration Guide(V7)*.

Command reference

See *HPE FlexNetwork MSR Routers IP Multicast Command Reference(V7)*.

Modified feature: 802.1X redirect URL

Feature change description

The value range for the *url-string* argument was changed to 1 to 256 characters for the **dot1x ead-assistant url** command.

Command changes

Modified command: dot1x ead-assistant url

Syntax

dot1x ead-assistant url *url-string*

Views

System view

Change description

Before modification: The value range for the *url-string* argument is 1 to 64 characters.

After modification: The value range for the *url-string* argument is 1 to 256 characters.

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Feature change description

The **source** *interface-type interface-number* option was added to the **display ntp-service trace** command.

Command changes

Modified command: **display ntp-service trace**

Old syntax

dot1x ead-assistant url *url-string*

New syntax

display ntp-service trace [**source** *interface-type interface-number*]

Views

Any view

Change description

The **source** *interface-type interface-number* option was added to the **display ntp-service trace** command.

Modified feature: Saving, rolling back, and loading the configuration

Feature change description

The following configuration guidelines were added when you use NETCONF to save, roll back, or load the configuration:

- The save, rollback, and load operations supplement NETCONF requests. Performing the operations might consume a lot of system resources.

- Multiple users are allowed to simultaneously perform the save, rollback, or load operation, but the result returned to each user might be inconsistent with the user request. Do not perform the save, rollback, or load operation when a lot of users are performing the operation.

Command changes

None

Modified feature: Displaying information about SSH users

Feature change description

In this release, the **display ssh user-information** command does not display the public key name for an SSH user that uses password authentication.

Command changes

Modified command: display ssh user-information

Syntax

```
display ssh user-information [ username ]
```

Views

Any view

Change description

Before modification: The **User-public-key-name** field in the command output displays **null** for an SSH user that uses password authentication.

After modification: The **User-public-key-name** field in the command output is blank for an SSH user that uses password authentication.

Removed feature: Displaying fabric utilization

Feature change description

The device does not support displaying switching fabric channel usage on interface cards.

Removed command

display fabric utilization

Syntax

In standalone mode:

display fabric utilization [**slot** *slot-number*]

In IRF mode:

display fabric utilization [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

ESS 0302P06

This release has the following changes:

New feature: Object policies

New feature: IPHC

New feature: Support of PPPoE server for IPv6

New feature: QSIG tunneling over SIP-T

New feature: Playout delay

New feature: BGP L2VPN support for NSR

New feature: BGP support for dynamic peers

New feature: ARP PnP

New feature: Support of Syslog for DNS and support of customlog&userlog for IPv6 hosts

New feature: QoS soft forwarding

New feature: Filtering by application layer protocol status

New feature: ADVPN support for multicast forwarding

New feature: MPLS LDP support for IPv6

New feature: Port security

New feature: Customizable IVR

New feature: SRST

New feature: NEMO

New feature: Support of MFR and FR for L2VPN, FR QoS, and FR compression and fragmentation

New feature: Support for LLDP on CPOS interfaces

New feature: SMS-based automatic configuration

New feature: ARP attack protection

New feature: SIP support for VRF

New feature: Object policies

Configuring Object policies

A zone pair has a source security zone and a destination security zone. ASPF uses zone pairs to identify the data flows to be examined. ASPF examines only received first data packets.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: IPHC

Configuring IPHC

The device supports PPP IPHC and frame relay IPHC.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Support of PPPoE server for IPv6

Configuring Support of PPPoE server for IPv6

On IPv6 networks, PPP negotiates only the IPv6 interface identifier instead of the IPv6 address and IPv6 DNS server address during IPv6CP negotiation.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: QSIG tunneling over SIP-T

Configuring QSIG tunneling over SIP-T

QSIG tunneling over SIP-T tunnels QSIG messages across a SIP network by encapsulating them in SIP message bodies. This feature enables ISDN networks to communicate over a SIP network.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Playout delay

Configuring Playout delay

By buffering incoming voice packets with different delay times for a period of time (playout delay time), the receiver can smoothly play out the voice packets to the codec. By configuring playout delay, you can prevent delay variation (jitter) from affecting voice quality.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: BGP L2VPN support for NSR

Configuring BGP L2VPN support for NSR

The active BGP process backs up BGP peers and routing information to the standby BGP process only when BGP NSR is enabled.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: BGP support for dynamic peers

Configuring BGP support for dynamic peers

The dynamic BGP peer feature enables BGP to establish dynamic BGP peer relationships with devices in a network. BGP accepts connection requests from the network. After a device in the network initiates a connection request, BGP establishes a dynamic peer relationship with the device.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: ARP PnP

Configuring ARP PnP

The ARP plug and play (PnP) feature allows end users to access the gateway without changing their IP addresses on subnets different from the subnet where the gateway resides.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Support of Syslog for DNS and support of customlog&userlog for IPv6 hosts

Configuring Support of Syslog for DNS and support of customlog&userlog for IPv6 hosts

The two flow log export destinations (information center and log host) are mutually exclusive. Only one export destination can be used at a time. If you configure both export destinations, the flow logs are exported to the information center and are not exported to the log host.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: QoS soft forwarding

Configuring QoS soft forwarding

- Configuring PQ: You can define a set of assignment rules in a PQ list and then apply the PQ list to an interface or PVC.
- Configuring CQ: You can configure a CQ list that contains up to 16 queues. The CQ list specifies the following information:
 - The queue where a packet is placed in.
 - The maximum length of each queue.
 - The number of bytes sent from the queue during a cycle of round robin scheduling.
- Configuring RTPQ.
- Configuring packet information pre-extraction: To process the original IP packets with QoS on the physical interface for a tunnel interface, configure packet information pre-extraction on the tunnel interface.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Filtering by application layer protocol status

Configuring Filtering by application layer protocol status

ASPF inspection supports protocol status validity check for application protocols of DNS, FTP, H323, HTTP, SCCP, SIP, and SMTP. ASPF drops packets with invalid protocol status.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: ADVPN support for multicast forwarding

Configuring ADVPN support for multicast forwarding

After NBMA mode is enabled on an ADVPN tunnel interface, the interface forwards multicast data only to spokes that need the data.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: MPLS LDP support for IPv6

Configuring MPLS LDP support for IPv6

LDP can operate on a pure IPv4 or IPv6 network or a network where IPv4 and IPv6 coexist. LDP operates similarly on IPv4 and IPv6 networks.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Port security

Configuring Port security

- **MAC move**—This feature allows 802.1X or MAC authenticated users to move from a port to another port on the device. The authentication session is deleted from the first port, and the users are reauthenticated on the new port.
- **SNMP notifications for port security**—This feature allows the port security module to generate SNMP notifications to report important events.
- **MAC authentication delay**—When both 802.1X authentication and MAC authentication are enabled on a port, you can delay MAC authentication so that 802.1X authentication is preferentially triggered. If no 802.1X authentication is triggered or 802.1X authentication fails within the delay period, the port continues to process MAC authentication.
- **VLAN assignment**—Both the 802.1X and MAC authentication features support VLAN assignment for users.
- **ACL assignment**—Both the 802.1X and MAC authentication features support ACL assignment for users. You can specify an authorization ACL for a user to control the user's access to network resources. After the user passes authentication, the authentication server (local or remote) assigns the authorization ACL to the access port of the user. The ACL will filter traffic for this user.
- **802.1X EAD assistant**—This feature allows unauthenticated 802.1X users to access the free IP. The feature also enables the device to redirect a user who is seeking to access the network to a specific URL on the free IP. For example, you can use this feature to redirect the user to the EAD client software download page.

- **802.1X SmartOn**—This feature was developed to support the NEC 802.1X client. The device performs SmartOn authentication before 802.1X authentication. If a user fails SmartOn authentication, the device stops 802.1X authentication for the user.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Customizable IVR

Configuring Customizable IVR

Interactive voice response (IVR) is extensively used in voice communications. The IVR system enables you to customize interactive operations and humanize other services. If a subscriber dials an IVR access number, the IVR system plays the prerecorded voice prompts to direct the subscriber about how to proceed.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: SRST

Configuring SRST

SRST provides call handling for a branch office when the branch office loses connectivity to the central voice server or the WAN connection is down. An SRST router in the branch office takes over to manage calls to ensure that local phones can make and receive calls. When the WAN connection is restored, call handling reverts back to the central voice server.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: NEMO

Configuring NEMO

As an extension of MIP, network mobility (NEMO) enables a node to retain the same IP address and maintain application connectivity when the node travels across networks. It allows location-independent routing of IP datagrams on the Internet. A mobile router is a router that operates as a mobile node connecting the mobile network and the home agent.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Support of MFR and FR for L2VPN, FR QoS, and FR compression and fragmentation

Configuring Support of MFR and FR for L2VPN, FR QoS, and FR compression and fragmentation

Frame Relay supports MPLS L2VPN and can then communicate with other networks through MPLS L2VPN. As a result, Layer 2 data can be transparently transmitted between Frame Relay networks through an MPLS or IP network.

When FRTS is disabled, only FR interface queues are in effect. The predefined FR PVC queues take effect only when FRTS is enabled.

The Frame Relay compression feature can compress Frame Relay packets to save bandwidth, reduce the network load, and improve the transmission efficiency for data in the Frame Relay network. The Frame Relay fragmentation feature can divide a large Frame Relay packet into several small packets, so that large packets can be transmitted over a low-speed link with a low delay.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: Support for LLDP on CPOS interfaces

Configuring Support for LLDP on CPOS interfaces

LLDP is supported on CPOS interfaces.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: SMS-based automatic configuration

Configuring SMS-based automatic configuration

Support for SMS-based automatic configuration. With SMS-based automatic configuration, the device can connect to an IMC server over a 3G or 4G network to obtain a configuration file.

To initiate SMS-based automatic configuration process, the administrator can use a cell phone or the IMC server to send a short message to the device. The IMC server sends short messages to devices through an SMS gateway. This feature can be used when the devices to be configured are widely distributed and there are 3G or 4G networks available for wireless communication.

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: ARP attack protection

Configuring ARP attack protection

None

Command reference

See *HPE FlexNetwork MSR Configuration Guides(V7)* and *HPE FlexNetwork MSR Command References(V7)*.

New feature: SIP support for VRF

Configuring SIP support for VRF

This feature enables a PE device to provide SIP services for a VPN instance. To enable this feature, you can associate the VPN instance with SIP on the PE device. The PE device uses the interface bound to the VPN instance as the source for sending SIP signaling and media streams.

Configuration guidelines

When you enable SIP support for VRF, follow these guidelines:

- You cannot associate a VPN instance with SIP or remove the association when a SIP service such as calling, registration, subscription, or the keepalive function is being used.
- The VPN instance to associate with SIP must be already created.

Configuration procedure

To enable SIP support for VRF:

Step	Command	Remarks
Enter system view.	system-view	N/A
Create a VPN instance.	ip vpn-instance <i>vpn-instance-name</i>	By default, no VPN instance exists.
Enter voice view.	voice-setup	N/A
Enter SIP view.	sip	N/A
Associate a VPN instance with SIP.	vpn-instance <i>vpn-instance-name</i>	By default, no VPN instance is associated with SIP.

Command reference

vpn-instance

Use **vpn-instance** to associate a VPN instance with SIP.

Use **undo vpn-instance** to remove the association.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

No VPN instance is associated with SIP.

Views

SIP view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The VPN instance to associate with SIP must be already created.

You cannot associate a VPN instance or remove the association when a SIP service is being used.

Examples

Associate the VPN instance **vpn-voice** with SIP.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] vpn-instance vpn-voice
```

Related commands

- **ip binding vpn-instance** (*MPLS Command Reference*)
- **ip vpn-instance** (*MPLS Command Reference*)

ESS 0102

This release has the following changes:

- [New feature: Portal authentication](#)
- [New feature: MSDP](#)
- [New feature: IPsec MIB and IKE MIB](#)
- [New feature: PoE](#)
- [New feature: CoPP software forwarding feature](#)
- [New feature: Configuring MPLS LDP FRR](#)
- [New feature: Enhanced routing features](#)

- [New feature: Python](#)
- [New feature: ATM](#)
- [New feature: DHCP MIB](#)

New feature: Portal authentication

Portal authentication controls user access to the Internet. Portal authenticates a user by the username and password the user enters on a portal authentication page. Therefore, portal authentication is also known as Web authentication. When portal authentication is deployed on a network, an access device redirects unauthenticated users to the website provided by a portal Web server. The users can access the resources provided by the website. If the users want to access the Internet, they must pass authentication on the website.

Portal authentication is classified into the following types:

- **Active authentication**—Users visit the authentication website provided by the portal Web server and enter their username and password for authentication.
- **Forced authentication**—Users visit other websites and are redirected to the portal authentication website for authentication.

Portal authentication flexibly imposes access control on the access layer and vital data entries. It has the following advantages:

- Replaces client software with convenient authentication pages.
- Provides ISPs with diversified management choices and extended functions. For example, the ISPs can place advertisements, provide community services, and publish information on the authentication page.
- Supports multiple authentication modes. For example, re-DHCP authentication implements a flexible address assigning scheme and saves public IP addresses. Cross-subnet authentication can authenticate users reside in subnets different from the access device.

The device support portal 2.0 and portal 3.0.

Command reference

See *HPE FlexNetwork MSR Command References(V7)*.

New feature: MSDP

Configuring MSDP

MSDP is an inter-domain multicast solution that addresses the interconnection of PIM-SM domains. It discovers multicast source information in other PIM-SM domains.

In the basic PIM-SM mode, a multicast source registers only with the RP in the local PIM-SM domain, and the multicast source information in each domain is isolated. As a result, both of the following occur:

- The RP obtains the source information only within the local domain.
- A multicast distribution tree is built only within the local domain to deliver multicast data locally.

MSDP enables the RPs of different PIM-SM domains to share their multicast source information. The local RP can then join the SPT rooted at the multicast source across the PIM-SM domains. This allows multicast data to be transmitted among different domains.

With MSDP peer relationships established between appropriate routers in the network, the RPs of different PIM-SM domains are interconnected with one another. These MSDP peers exchange source active (SA) messages, so that the multicast source information is shared among these domains.

For more information about configuring MSDP, see "MSDP Configuration Guide" in *HPE FlexNetwork MSR Configuration Guides(V7)*.

Command reference

See *HPE FlexNetwork MSR Command References(V7)*.

New feature: IPsec MIB and IKE MIB

IPsec-Monitor-MIB (HH3C-IPSEC-MONITOR-V2-MIB) monitors IPsec tunnels. NMS can use this MIB to obtain IPsec tunnel information, including algorithms, gateway addresses, and tunnel statistics. Except the trap function, all nodes of this MIB are read only.

Ike-Monitor-MIB (HH3C-IKE-MONITOR-MIB) monitors IKE tunnels. NMS can use this MIB to obtain IKE tunnel information.

For more information, see the MIB companion document.

New feature: PoE

Configuring PoE

IEEE 802.3af-compliant power over Ethernet (PoE) enables a power sourcing equipment (PSE) to supply power to powered devices (PDs) through Ethernet interfaces over twisted pair cables. Examples of PDs include IP telephones, wireless APs, portable chargers, card readers, Web cameras, and data collectors. A PD can also use a different power source from the PSE at the same time for power redundancy.

For more information about configuring PoE, see "PoE Configuration Guide" in *HPE FlexNetwork MSR Configuration Guides(V7)*.

Command reference

See *HPE FlexNetwork MSR Command References(V7)*.

New feature: CoPP software forwarding feature

Configuring CoPP

If the rate of packets sent to the control plane exceeds the processing capabilities of the control plane (for example, when the device is suffering DoS attacks), the normal packets sent to the control plane cannot be promptly processed, thus affecting the normal operation of protocols.

To protect the management interface against DoS attacks, which will cause service interruption, you must perform traffic policing for the management interface.

CoPP allows you to perform traffic policing for the control plane or management interface control plane. By default, the predefined QoS parameters are configured for packets of each protocol sent to the control plane. Also, you can apply a user-defined QoS policy to the control plane to filter and rate-limit the packets sent to the control plane. This makes sure the control plane can correctly receive, transmit, and process packets.

Command reference

control-plane

Use **control-plane** to enter control plane view.

Syntax

MSR2000 / MSR3000:

control-plane

MSR4000:

control-plane slot *slot-number*

Views

System view

Predefined user roles

network-admin

Examples

(MSR2000 / MSR3000.) Enter control plane view.

```
<Sysname> system-view  
[Sysname] control-plane  
[Sysname-cp]
```

(MSR4000.) Enter control plane view of the card in slot 3.

```
<Sysname> system-view  
[Sysname] control-plane slot 3  
[Sysname-cp-slot3]
```

control-plane management

❗ IMPORTANT:

A QoS policy applied to the management interface control plane takes effect on the packets sent from the management interface to the control plane.

Use **control-plane management** to enter management interface control plane view.

Syntax

control-plane management

Views

System view

Predefined user roles

network-admin

Examples

Enter management interface control plane view.

```
<Sysname> system-view  
[Sysname] control-plane management  
[Sysname-cp-management]
```

qos apply policy (interface view, control plane view)

❗ IMPORTANT:

A QoS policy applied to the management interface control plane takes effect on the packets sent from the management interface to the control plane.

Use **qos apply policy** to apply a QoS policy to an interface, a control plane.

Use **undo qos apply policy** to remove a QoS policy from an interface, a control plane.

Syntax

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

Default

No QoS policy is applied to an interface, a control plane, or a management interface control plane.

Views

Interface view, control plane view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming traffic of an interface, a control plane, or a management interface control plane.

outbound: Applies the QoS policy to the outgoing traffic of an interface.

Usage guidelines

To successfully apply a QoS policy to an interface, make sure the total bandwidth assigned to AF and EF queues in the QoS policy is smaller than the available bandwidth of the interface. If you modify the available bandwidth of the interface to a value smaller than the total bandwidth for AF and EF queues, the applied QoS policy is removed. For a QoS policy to be applied in the inbound direction, the referenced traffic behaviors cannot be configured with any of the commands **queue af**, **queue ef**, **queue wfq**, and **gts**.

When you apply a QoS policy to an interface, follow these guidelines:

- You can apply a QoS policy configured with various QoS actions (such as **remark**, **car**, **gts**, **queue af**, **queue ef**, **queue wfq**, and **wred**) to common physical interfaces.
- An inbound QoS policy cannot contain a GTS action or any of these queuing actions **queue ef**, **queue af**, or **queue wfq**.

Examples

Apply the QoS policy named **USER1** to the outgoing traffic of GigabitEthernet 0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 0/1
```

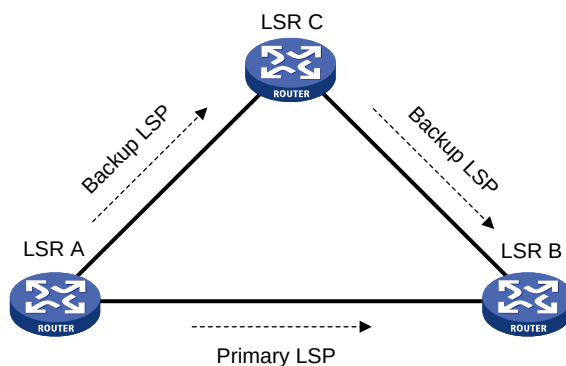
```
[Sysname-GigabitEthernet0/1] qos apply policy USER1 outbound
```

New feature: Configuring MPLS LDP FRR

Configuring MPLS LDP FRR

A link or router failure on a path can cause packet loss until LDP completes LSP establishment on the new path. LDP FRR enables fast rerouting to minimize the failover time. LDP FRR bases on IP FRR and is enabled automatically after IP FRR is enabled.

Figure 12 Network diagram for LDP FRR



In Figure 1, configure IP FRR on LSR A by using IGP to calculate or specify a backup next hop. LDP creates a primary LSP and a backup LSP according to the primary route and the backup route calculated by IGP. When the primary LSP operates correctly, it forwards the MPLS packets. When the primary LSP fails, LDP directs packets to the backup LSP.

When packets are forwarded through the backup LSP, IGP calculates the optimal path based on the new network topology. When IGP route convergence occurs, LDP establishes a new LSP according to the optimal path. If a new LSP is not established after IGP route convergence, traffic forwarding might be interrupted. Therefore, HPE recommends that you enable LDP IGP synchronization to work with LDP FRR to reduce the traffic interruption time.

Command reference

igp sync delay

Use **igp sync delay** to configure the delay for LDP to notify IGP of the LDP convergence completion.

Use **undo igp sync delay** to restore the default.

Syntax

igp sync delay *time*

undo igp sync delay

Default

LDP immediately notifies IGP of the LDP convergence completion.

Views

LDP view

Predefined user roles

network-admin

Parameters

time: Specifies the notification delay in the range of 5 to 300 seconds.

Usage guidelines

LDP convergence on a link is completed when the followings occur:

- The local device establishes an LDP session to at least one peer, and the LDP session is already in **Operation** state.
- The local device has distributed the label mappings to at least one peer.

MPLS traffic forwarding might be interrupted in one of the following scenarios:

- When the peer uses the **Ordered** label distribution control mode, the local device needs to wait for a label mapping from its downstream LSR after the LDP session goes into **Operation** state. If LDP immediately notifies IGP of the LDP convergence completion when the label mapping from downstream is not received, MPLS traffic forwarding might be interrupted.
- When a large number of label mappings are distributed from downstream, if LDP immediately notifies IGP of the LDP convergence completion, label advertisement might not be finished, and MPLS traffic forwarding is interrupted.

In these scenarios, you must use this command to configure the notification delay. When LDP convergence on a link is completed, LDP waits a delay time to notify IGP of the LDP convergence completion to reduce the traffic interruption time.

Examples

Configure the notification delay as 30 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] igp sync delay 30
```

Related commands

- **igp sync delay on-restart**
- **mpls ldp igp sync disable**
- **mpls ldp sync** (IS-IS view)
- **mpls ldp sync** (OSPF view/OSPF area view)

igp sync delay on-restart

Use **igp sync delay on-restart** to configure the maximum delay for LDP to notify IGP of the LDP IGP synchronization status after an LDP restart or an active/standby switchover occurs.

Use **undo igp sync delay on-restart** to restore the default.

Syntax

igp sync delay on-restart *time*

undo igp sync delay on-restart

Default

The maximum notification delay is 90 seconds.

Views

LDP view

Predefined user roles

network-admin

Parameters

time: Specifies the maximum notification delay in the range of 60 to 600 seconds.

Usage guidelines

After LDP restarts or an active/standby switchover occurs, LDP convergence begins after a period of time. If LDP immediately notifies IGP of all the current LDP IGP synchronization status, and updates the status after LDP convergence, IGP might frequently process the status, and the cost might increase.

The notification delay mechanism for an LDP restart or an active/standby switchover provides a notification delay of LDP process levels. When LDP restarts or an active/standby switchover occurs, this mechanism enables LDP to wait a period of time till LDP recovers to the status before the restart or switchover, and then notify IGP of the LDP IGP synchronization status in bulk. If LDP does not recover to the status before the restart or switchover when the maximum delay set by this command expires, LDP immediately notifies IGP of the LDP IGP synchronization status in bulk.

Examples

Configure the maximum notification delay as 300 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] igp sync delay on-restart 300
```

Related commands

- **igp sync delay**
- **mpls ldp igp sync disable**
- **mpls ldp sync** (IS-IS view)
- **mpls ldp sync** (OSPF view/OSPF area view)

mpls ldp igp sync disable

Use **mpls ldp igp sync disable** to disable LDP IGP synchronization on an interface.

Use **undo mpls ldp igp sync disable** to restore the default.

Syntax

mpls ldp igp sync disable

undo mpls ldp igp sync disable

Default

LDP IGP synchronization is enabled on an interface.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

After you enable LDP IGP synchronization for IGP, for example, an OSPF area or an IS-IS process, LDP IGP synchronization is enabled on the OSPF interfaces and IS-IS interfaces. To disable LDP IGP synchronization on an interface, execute the **mpls ldp igp sync disable** command on that interface.

Examples

Enable LDP IGP synchronization on GigabitEthernet 0/1.

```
<Sysname> System-view
[Sysname] interface gigabitethernet 0/1
[Sysname-GigabitEthernet0/1] mpls ldp igp sync disable
```

Related commands

- **mpls ldp sync** (IS-IS view)
- **mpls ldp sync** (OSPF view/OSPF area view)

New feature: Enhanced routing features

Configuring enhanced routing features

This release supports RIB NSR, IPv4 static route FRR, direct route redistribution, and RFC4382 MIB (MPLS-L3VPN-STD-MIB).

Command reference

non-stop-routing

Use **non-stop-routing** to enable RIB NSR to back up routing information.

Use **undo non-stop-routing** to restore the default.

Syntax

non-stop-routing

undo non-stop-routing

Default

RIB NSR is disabled.

Views

RIB IPv4 address family view, RIB IPv6 address family view

Predefined user roles

network-admin

Examples

```
# Enable NSR for the RIB IPv4 address family.  
<Sysname> system-view  
[Sysname] rib  
[Sysname-rib] address-family ipv4  
[Sysname-rib-ipv4] non-stop-routing
```

ip route-static fast-reroute auto

Use **ip route-static fast-reroute auto** to configure static route FRR to automatically select a backup next hop.

Use **undo ip route-static fast-reroute auto** to disable static route FRR.

Syntax

ip route-static fast-reroute auto

undo ip route-static fast-reroute auto

Default

Static route FRR is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Configure static route FRR to automatically select a backup next hop.

```
<Sysname> system-view
[Sysname] ip route-static fast-reroute auto
```

import-route (RIP view)

Use **import-route** to enable route redistribution from another routing protocol.

Use **undo import-route** to disable route redistribution.

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route *protocol* [*process-id* | **all-processes**]

Default

RIP does not redistribute routes from any other routing protocol.

Views

RIP view

Predefined user roles

network-admin

Parameters

protocol: Specifies a routing protocol from which RIP redistributes routes. It can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1. This argument is available only when the protocol is **isis**, **rip**, or **ospf**.

all-processes: Enables route redistribution from all the processes of the specified protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows redistribution of IBGP routes. This keyword is available when the *protocol* argument is set to **bgp**.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost*: Specifies a cost for redistributed routes, in the range of 0 to 16. The default cost is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag for marking redistributed routes, in the range of 0 to 65535. The default is 0.

Usage guidelines

The **import-route bgp** command redistributes only EBGp routes. The **import-route bgp allow-ibgp** command additionally redistributes IBGP routes and might cause routing loops. Therefore, use it with caution.

This command redistributes only active routes. To view route state information, use the **display ip routing-table protocol** command.

The **undo import-route protocol all-processes** command removes only the configuration made by the **import-route protocol all-processes** command, instead of the configuration made by the **import-route protocol process-id** command.

Examples

Redistribute static routes into RIP, and set the cost for redistributed routes to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Related commands

default cost

import-route (OSPF view)

Use **import-route** to redistribute AS-external routes from another routing protocol.

Use **undo import-route** to disable route redistribution from another routing protocol.

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route *protocol* [*process-id* | **all-processes**]

Default

OSPF does not redistribute AS-external routes from any other routing protocol.

Views

OSPF view

Predefined user roles

network-admin

Parameters

protocol: Redistributes routes from the specified protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1. It is available only when the *protocol* is **rip**, **ospf**, or **isis**.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Redistributes IBGP routes. It is available only when the *protocol* is **bgp**.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost cost: Specifies a route cost in the range of 0 to 16777214. The default is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the router is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name*: Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag tag: Specifies a tag for marking external LSAs, in the range of 0 to 4294967295. The default is 1.

type type: Specifies a cost type, 1 or 2. The default is 2.

Usage guidelines

This command redistributes routes destined for other ASs from another protocol. AS external routes include the following types:

- Type-1 external route
- Type-2 external route

A Type-1 external route has high reliability. Its cost is comparable with the cost of OSPF internal routes. The cost from an OSPF router to a Type-1 external route's destination equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.

A Type-2 external route has low credibility. OSPF considers the cost from the ASBR to the destination of a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. The cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command cannot redistribute default external routes.

The **import-route bgp** command redistributes only EBGP routes. Because the **import-route bgp allow-ibgp** command redistributes both EBGP and IBGP routes and might cause routing loops, use it with caution.

Only active routes can be redistributed. To view information about active routes, use the **display ip routing-table protocol** command.

The **undo import-route protocol all-processes** command removes only the configuration made by the **import-route protocol all-processes** command, instead of the configuration made by the **import-route protocol process-id** command.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

Examples

Redistribute routes from RIP process 40 and specify the type, tag, and cost as 2, 33, and 50 for redistributed routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

Related commands

default-route-advertise (OSPF view)

import-route (IS-IS view)

Use **import-route** to redistribute routes from another routing protocol or another IS-IS process.

Use **undo import-route** to remove the redistribution.

Syntax

import-route protocol [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost cost** | **cost-type** { **external** | **internal** }] [**level-1** | **level-1-2** | **level-2**] [**route-policy route-policy-name** | **tag tag**] *

undo import-route protocol [*process-id* | **all-processes**]

Default

No route redistribution is configured.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

protocol: Redistributes routes from a routing protocol, which can be BGP, direct, IS-IS, OSPF, RIP, or static.

process-id: Specifies a process by its ID in the range of 1 to 65535. It is available only when the protocol is **isis**, **ospf**, or **rip**.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows redistribution of IBGP routes. It is available when the protocol is BGP.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost: Specifies a cost for redistributed routes, which is in the range of 0 to 4261412864.

- For the styles of **narrow**, **narrow-compatible**, and **compatible**, the cost is in the range of 0 to 63.
- For the styles of **wide** and **wide-compatible**, the cost is in the range of 0 to 4261412864.

cost-type { external | internal }: Specifies the cost type. The **internal** type indicates internal routes, and the **external** type indicates external routes. If **external** is specified, the cost of a redistributed route is added by 64 to make internal routes take priority over external routes. The type is **external** by default. The keywords are available only when the cost type is **narrow**, **narrow-compatible**, or **compatible**.

level-1: Redistributes routes into the Level-1 routing table.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

route-policy *route-policy-name*: Redistributes only routes matching the specified routing policy. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag *tag*: Specifies a tag value for marking redistributed routes, in the range of 1 to 4294967295.

Usage guidelines

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

The effective cost depends on the cost style. For the styles of **narrow**, **narrow-compatible**, and **compatible**, the cost is in the range of 0 to 63. If the cost is more than 63, 63 is used. For the style of **wide** or **wide-compatible**, the configured value is the effective value.

This **import-route** command cannot redistribute default routes. The command redistributes only active routes. To display route state information, use the **display ip routing-table protocol** command.

The **import-route bgp** command redistributes only EBGP routes.

The **import-route bgp allow-ibgp** command redistributes both EBGP and IBGP routes. Because this command might cause routing loops, use it with caution.

The **undo import-route protocol all-processes** command removes only the configuration made by the **import-route protocol all-processes** command, instead of the configuration made by the **import-route protocol process-id** command.

Examples

Redistribute static routes into IS-IS, and set the cost for redistributed routes to 15.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] import-route static cost 15
```

Related commands

import-route limit

import-route (BGP view)

Use **import-route** to enable BGP to redistribute routes from an IGP protocol.

Use **undo import-route** to disable route redistribution from an IGP protocol.

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view:

```
import-route protocol [ { process-id | all-processes } [ allow-direct | med med-value | route-policy route-policy-name ] * ]
```

```
undo import-route protocol [ process-id | all-processes ]
```

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view:

```
import-route protocol [ process-id [ allow-direct | med med-value | route-policy route-policy-name ] * ]
```

```
undo import-route protocol [ process-id ]
```

Default

BGP does not redistribute IGP routes.

Views

BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view

Predefined user roles

network-admin

Parameters

protocol: Redistributes routes from a specified IGP protocol. In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view, it can be **direct**, **isis**, **ospf**, **rip**, or **static**. In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view, it can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1. In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view, it is available only when the protocol is **isis**, **ospf**, or **rip**. In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view, it is available only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

all-processes: Redistributes routes from all the processes of the specified IGP protocol. This keyword takes effect only when the protocol is **isis**, **ospf**, or **rip**.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy route-policy-name** option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

med med-value: Specifies a MED value for redistributed routes, in the range of 0 to 4294967295. If no MED is specified, the metric of a redistributed route is used as its MED.

route-policy route-policy-name: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes or set route attributes for redistributed routes.

Usage guidelines

The **import-route** command cannot redistribute default IGP routes. To redistribute default IGP routes, use the **default-route imported** command together with the **import-route** command.

Only active routes can be redistributed. You can use the **display ip routing-table protocol** or **display ipv6 routing-table protocol** command to view route state information.

The ORIGIN attribute of routes redistributed by the **import-route** command is INCOMPLETE.

Examples

In BGP IPv4 unicast address family view, redistribute routes from RIP process 1, and set the MED value for redistributed routes to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] address-family ipv4 unicast
[Sysname-bgp-ipv4] import-route rip 1 med 100
```

In BGP-VPN IPv4 unicast address family view, redistribute routes from RIP process 1, and reference a routing policy **imprt** to exclude route 1.1.1.0/24 from route redistribution.

```
<Sysname> system-view
[Sysname] ip prefix-list imprt deny 1.1.1.0 24
[Sysname] ip prefix-list imprt permit 0.0.0.0 0 less-equal 32
[Sysname] route-policy imprt permit node 0
[Sysname-route-policy-imprt-0] if-match ip address prefix-list imprt
[Sysname-route-policy-imprt-0] quit
[Sysname] bgp 100
[Sysname-bgp] ip vpn-instance vpn1
[Sysname-bgp-vpn1] address-family ipv4 unicast
[Sysname-bgp-ipv4-vpn1] import-route rip 1 route-policy imprt
```

In BGP IPv6 unicast address family view, redistribute routes from RIP process 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] address-family ipv6 unicast
[Sysname-bgp-ipv6] import-route ripng
```

In BGP-VPN IPv6 unicast address family view, redistribute routes from RIP process 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ip vpn-instance vpn1
[Sysname-bgp-vpn1] address-family ipv6 unicast
[Sysname-bgp-ipv6-vpn1] import-route ripng
```

Related commands

- **display ip routing-table protocol**
- **display ipv6 routing-table protocol**

import-route (RIPng view)

Use **import-route** to redistribute routes from another routing protocol.

Use **undo import-route** to disable route redistribution.

Syntax

import-route *protocol* [*process-id*] [**allow-ibgp**] [**allow-direct** | **cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

Default

RIPng does not redistribute routes from another routing protocol.

Views

RIPng view

Predefined user roles

network-admin

Parameters

protocol: Specifies a routing protocol from which RIPng redistributes routes. It can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Specifies a process by its ID in the range of 1 to 65535. The default is 1. This argument is available only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

allow-ibgp: Allows redistribution of IBGP routes. This keyword is available when the *protocol* argument is set to **bgp4+**.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the

allow-direct keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost*: Specifies a metric for redistributed routes, in the range of 0 to 16. The default metric is 0.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes.

Examples

Redistribute routes from IPv6 IS-IS process 7 into RIPng and set the metric for redistributed routes to 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

import-route (OSPFv3 view)

Use **import-route** to redistribute routes.

Use **undo import-route** to disable route redistribution.

Syntax

import-route *protocol* [*process-id* | **all-processes** | **allow-ibgp**] [**allow-direct** | **cost** *cost* | **nssa-only** | **route-policy** *route-policy-name* | **tag** *tag* | **type** *type*] *

undo import-route *protocol* [*process-id* | **all-processes**]

Default

OSPFv3 route redistribution is disabled.

Views

OSPFv3 view

Predefined user roles

network-admin

Parameters

protocol: Redistributes routes from the specified routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Specifies the process ID of a routing protocol, in the range of 1 to 65536. It defaults to 1. This argument takes effect only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

all-processes: Redistributes routes from all the processes of the specified routing protocol. This keyword takes effect only when the protocol is **ripng**, **ospfv3**, or **isisv6**.

allow-ibgp: Redistributes IBGP routes. It is available only when the protocol is **bgp4+**.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost cost: Specifies a cost for redistributed routes, in the range of 1 to 16777214. The default is 1.

nssa-only: Limits the route advertisement to the NSSA area by setting the P-bit of Type-7 LSAs to 0. By default, the P-bit of Type-7 LSAs is set to 1. If the router acts as both an ASBR and an ABR and **FULL** state neighbors exist in the backbone area, the P-bit of Type-7 LSAs originated by the router is set to 0. This keyword applies to NSSA routers.

route-policy *route-policy-name:* Specifies a routing policy to filter redistributed routes. The *route-policy-name* argument is a case-sensitive string of 1 to 63 characters.

tag tag: Specifies a tag for marking external LSAs, in the range of 0 to 4294967295. If this option is not specified, no tag is contained in advertised LSAs by default.

type type: Specifies the type for redistributed routes, 1 or 2. The default is 2.

Usage guidelines

An external route is a route to a destination outside the OSPFv3 AS. External routes types are as follows:

- A Type-1 external route has high reliability. Its cost is comparable with the cost of OSPFv3 internal routes. The cost from an OSPFv3 router to a Type-1 external route's destination equals the cost from the router to the ASBR plus the cost from the ASBR to the external route's destination.
- A Type-2 external route has low credibility, so OSPFv3 considers the cost from the ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPFv3 internal router. The cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

The **import-route** command cannot redistribute default routes.

The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes both EBGP and IBGP routes, and might cause routing loops. Therefore, use it with caution.

The **import-route nssa-only** command redistributes AS-external routes in Type-7 LSAs only into the NSSA area.

Examples

Configure OSPFv3 process 1 to redistribute routes from RIPv3 and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes discovered by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

ipv6 import-route (IPv6 IS-IS view)

Use **ipv6 import-route** to enable IPv6 IS-IS to redistribute routes from another routing protocol.

Use **undo ipv6 import-route** to disable route redistribution.

Syntax

ipv6 import-route *protocol* [*process-id*] [**allow-ibgp**] [**allow-direct** | **cost** *cost* | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo ipv6 import-route *protocol* [*process-id*]

Default

IPv6 does not redistribute routes from any other routing protocol.

Views

IS-IS view

Predefined user roles

network-admin

Parameters

protocol: Redistributes routes from the specified routing protocol, which can be **direct**, **static**, **ripng**, **isisv6**, **bgp4+**, or **ospfv3**.

process-id: Specifies a process by its ID in the range of 1 to 65535. It is available only when the protocol is **ripng**, **isisv6**, or **ospfv3**.

allow-direct: Redistributes the networks of the local interfaces enabled with the specified routing protocol. By default, the networks of the local interfaces are not redistributed. If you specify both the **allow-direct** keyword and the **route-policy** *route-policy-name* option, make sure the **if-match** rule defined in the routing policy does not conflict with the **allow-direct** keyword. For example, if you specify the **allow-direct** keyword, do not configure the **if-match route-type** rule for the routing policy. Otherwise, the **allow-direct** keyword does not take effect.

cost *cost*: Specifies a cost for redistributed routes, in the range of 0 to 4261412864.

level-1: Redistributes routes into the Level-1 routing table.

level-1-2: Redistributes routes into Level-1 and Level-2 routing tables.

level-2: Redistributes routes into the Level-2 routing table.

route-policy *route-policy-name*: Specifies a routing policy by its name, a case-sensitive string of 1 to 63 characters, to filter redistributed routes.

tag *tag*: Specifies an administrative tag for marking redistributed routes, in the range of 1 to 4294967295.

allow-ibgp: Allows redistribution of IBGP routes. This keyword is available only when the protocol is **bgp4+**.

Usage guidelines

IPv6 IS-IS considers redistributed routes as AS-external routes.

You can specify a cost and a level for redistributed routes.

The **import-route bgp4+** command redistributes only EBGp routes. The **import-route bgp4+ allow-ibgp** command redistributes both EBGp and IBGP routes, and might cause routing loops. Therefore, use it with caution.

Examples

Configure IPv6 IS-IS to redistribute static routes and set the cost for redistributed routes to 15.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 import-route static cost 15
```

New feature: Python

Using Python

Python is an easy to learn, powerful programming language. It has efficient high-level data structures and a simple but effective approach to object-oriented programming. Python's elegant syntax and dynamic typing, together with its interpreted nature, make it an ideal language for scripting and rapid application development in many areas on most platforms.

Comware V7 provides a built-in Python interpreter that supports the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- Comware V7 extended API.
- Python scripts. You can use a Python script to configure the system automatically.

To use Python 2.7 commands and the APIs, you must enter the Python shell.

Command reference

See *HPE FlexNetwork MSR Command References(V7)*.

New feature: ATM

Configuring ATM

Asynchronous Transfer Mode (ATM) is a technology based on packet transmission mode while incorporating the high-speed of circuit transmission mode. ATM was adopted as the transmission and switching mode for broadband ISDN by the ITU-T in June 1992. Due to its flexibility and support for multimedia services, ATM is regarded as core broadband technology.

As defined by the ITU-T, data is encapsulated in cells in ATM. Each ATM cell is 53 bytes in length, of which the first five bytes contain cell header information and the last 48 bytes contain payload. The major function of the cell header is to identify virtual connection. In addition, it can be used to carry limited flow control, congestion control, and error control information.

Command reference

See *HPE FlexNetwork MSR Command References(V7)*.

New feature: DHCP MIB

DHCP MIB

The MIB supports HH3C-DHCP4-MIB and HH3C-DHCP-SNOOP2-MIB. For more information about MIB nodes, see the MIB companion document.

Command reference

if-match

Use **if-match** to configure a match rule for a DHCP user class.

Use **undo if-match** to remove the match rule for a DHCP user class.

Syntax

if-match rule rule-number option option-code [hex hex-string [mask mask | offset offset length length]]

undo if-match rule rule-number

Syntax

No match rule is configured for the DHCP user class.

Views

DHCP user class view

Predefined user roles

network-admin

Parameters

rule *rule-number*: Assigns the match rule an ID in the range of 1 to 16. A smaller ID represents a higher match priority.

option *option-code*: Matches a DHCP option by a number in the range of 1 to 254.

hex *hex-string*: Matches the specified string in the option, which must be a hex string of even numbers in the range of 2 to 256. If you do not specify the *hex-string* argument, the DHCP server only checks whether the specified option exists in the received packets.

mask *mask*: Specifies the mask used to match the option content. The *mask* argument is a hex string of even numbers in the range of 2 to 256. The length of *mask* must be the same as that of *hex-string*.

offset *offset*: Specifies the offset to match the option, in the range of 0 to 254 bytes. If you do not specify the *offset* argument, the server matches the entire option with the rule.

length *length*: Matches the specified length of the option, in the range of 1 to 128 bytes. The specified length must be the same as the *hex-string* length.

Usage guidelines

You can configure multiple match rules for a DHCP user class. Each match rule is uniquely identified by a rule ID. Different match rules can include the same option code, but they cannot have the exact same matching criteria.

The DHCP server matches DHCP requests against the match rules. A DHCP client matches a DHCP user class when its request matches one of the specified match rules.

The match operation follows these guidelines:

- If only the *option-code* argument is specified in the rule, packets containing the option match the rule.
- If only the *option-code* and *hex-string* arguments are specified in the rule, packets that have the specified hex string in the specified option match the rule.
- If the *option-code*, *hex-string*, *offset* and *length* arguments are specified in the rule, packets match the rule as long as their content from offset+1 bit to offset+length bit in the specified option is the same as the specified hex string.
- If the *option-code*, *hex-string*, and *mask* arguments are specified in the rule, the DHCP server ANDs the content from the first bit to the mask-1 bit in the specified option with the mask, and

then compares the result with the result of the AND operation between *hex-string* and *mask*. If the two results are the same, the received packet matches the rule.

Examples

Configure match rule **1** to match DHCP requests that contain Option 82 for DHCP user class **contain-option82**.

```
<Sysname> system-view
[Sysname] dhcp class contain-option82
[Sysname-dhcp-class-contain-option82] if-match rule 1 option 82
```

Configure match rule **2** to match DHCP requests that contain Option 82 whose first three bytes is **0x13ae92** for DHCP user class **exam**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 2 option 82 hex 13ae92 offset 0 length 3
```

Configure match rule **3** to match DHCP requests that contain Option 82 whose highest bit of the fourth byte is 1 for DHCP user class **exam**.

```
<Sysname> system-view
[Sysname] dhcp class exam
[Sysname-dhcp-class-exam] if-match rule 3 option 82 hex 00000080 mask 00000080
```

Related commands

dhcp class

ESS 0006P02

None