Hewlett Packard Enterprise

HPE 5510HI-CMW710-R3507-US Release Notes

Contents

List of tables

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version 5510HI-CMW710-R3507-US. In the interest of brevity, any reference to R3507 is also applicable to R3507-US for the remainder of this document. Before you use this version on 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 5510HI-CMW710-R3507-US Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 3507

Note: You can see the version number with the command **display version** in any view. Please see **Note①**.

Version history

IMPORTANT:

The software feature changes listed in the version history table for each version are not complete. To obtain complete information about all software feature changes in each version, see the *Software Feature Changes* document for this release notes.

Table 1 Version history

Version number	Last version	Release Date	Release type	Remarks
R3507-US	R3506P11	2021-06-08	Release version	This version fixed bugs and introduced feature changes. New features include: • EAD assistant
R3506P11	R3506P10	2021-01-29	Release version	This version fixed bugs.

Version number	Last version	Release Date	Release type	Remarks
R3506P10	R3506P08	2020-11-13	Release version	This version fixed bugs and introduced feature changes. New features include: • Configuring the 802.1p priority for control packets sent by a device • Packet spoofing logging and filtering entry logging for SAVI • Configuring password control over weak passwords • Enabling password change prompt logging • Enabling recording untrusted DHCP servers on a DHCP snooping device There are also modified features.
R3506P08	R3506P06	2020-07-27	Release version	This version fixed bugs.
R3506P06	R3506P03	2020-06-19	Release version	This version fixed bugs and introduced feature changes. New features include: • Enabling recording untrusted DHCP servers on a DHCP snooping device There are also modified features.
R3506P03	R3506P02	2020-03-24	Release version	This version fixed bugs.
R3506P02	R3506P01	2019-12-23	Release version	This version fixed bugs.
R3506P01	R3506	2019-10-31	Release version	This version fixed bugs.
R3506	R1311P02	2019-07-12	Release version	
R1311P02	R1311P01	2019-02-20	Release version	This version fixed bugs.
R1311P01	R1309P07	2018-12-26	Release version	This version fixed bugs and introduced feature changes. New features include: • Specifying DNS server information in RA messages • Specifying DNS suffix information in RA messages • Suppressing advertising DNS information in RA messages • HTTP redirect There are also modified features. Fixed bugs

Version number	Last version	Release Date	Release type	Remarks
R1309P07	R1309P06	2018-09-26	Release version	This version fixed bugs and introduced feature changes. New features include: • Automatic obtaining of the login username for temporary user role authorization • 802.1X EAP-TLS fragmentation for packets sent to the server There are also modified features. Fixed bugs
R1309P06	R1309P03	2018-08-02	Release version	This version fixed bugs and introduced feature changes. New features include: • Enabling interface consistency check for ARP and MAC address entries • 802.1X offline detection There are also modified features. Fixed bugs
R1309P03	R1309	2018-04-27	Release version	This version fixed bugs and introduced feature changes. New features include: • PD detection mode • 802.1X user logging • MAC authentication user logging • Port security user logging • Configuring the Event MIB Removed feature: • Enabling PoE for a PSE
R1309	R1308	2017-08-15	Release version	This version fixed bugs and introduced feature changes. New features include: • MAC address information display for 802.1X users in 802.1X VLANs of a specific type • Authorization CAR action in an ISP domain • 802.1X client There are also modified features. Fixed bugs
R1308	R1121P03	2017-03-07	Release version	• Added new feature See the *Software Feature Changes* document for this release notes.

Version number	Last version	Release Date	Release type	Remarks
R1121P03	R1121P02	2016-12-22	Release version	New feature: • Link aggregation management VLANs and management port • ISP domain for users assigned to nonexistent domains Modified feature: • Maximum length of jumbo frames allowed by an Ethernet interface • Username format modification for device login Fixed bugs
R1121P02	R1121P01	2016-11-25	Release version	Fixed bugs
R1121P01	R1121	2016-10-27	Release version	New feature: • SSH listening port Fixed bugs
R1121	R1120P10	2016-09-08	Release version	Modified feature: • Specifying log hosts Fixed bugs
R1120P10	R1120P07	2016-07-11	Release version	New feature: • 802.1X critical voice VLAN • MAC authentication critical voice VLAN • MAC authentication support for Session-Timeout and Termination-Action attributes • Enabling SNMP notifications for port security Modified feature: • CDP enhancement • Configuring a test profile for RADIUS server status detection • NTP support for ACL • Storm control for known unicast packets Fixed bugs
R1120P07	R1120	2016-05-19	Release version	• Modified feature: • NTP authentication • Display Mac address entries • Fixed bugs

Version number	Last version	Release Date	Release type	Remarks
R1120	R1118P02	2016-03-13	Release version	New feature: • Specifying ITU channel numbers for transceiver modules • ISSU • Configuring the DHCP smart relay feature • RADIUS server status detection • RADIUS server load sharing • Sending EAP-Success packets to 802.1X users in critical VLAN • ND Snooping • ND attack detection • RA guard • Setting port security's limit on the number of secure MAC addresses for specific VLANs Modified feature: • Maximum number of secure MAC addresses on a port for port security • Specifying RADIUS servers Fixed bugs
R1118P02	R1118	2015-12-30	Release version	New feature: • MACsec Fixed bugs
R1118	R1111P01	2015-12-08	Release version	New feature: • Disable SSL session renegotiation for the SSL server • IPsec support for Suite B • SSH support for Suite B • Public key management support for Suite B • PKI support for Suite B • SSL support for Suite B Modified feature: • FIPS self-tests Fixed bugs
R1111P01	First release	2015-03-31	Release version	First release

Hardware and software compatibility matrix

CAUTION:

To avoid an upgrade failure, use Table 2 to verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	5510HI Series
Hardware platform	HPE 5510 24G 4SFP+ HI 1-slot Switch JH145A HPE 5510 48G 4SFP+ HI 1-slot Switch JH146A HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch JH147A HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch JH148A HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A
Minimum memory requirements	2 GB
Minimum Flash requirements	512 M
Boot ROM version	Version 128 or higher (Note: Use the **display version** command in any view to view the version information. Please see **Note②**)
Host software & SHA 256 Checksum	5510HI-CMW710-R3507-US.ipe 17f26f38a13b040f88d590b734f9d41ab6f65ed730e12856344542f0f42245ad 5510hi-cmw710-packet-capture-r3507-US.bin dce80a648f125e58a975c8650266a64e4cb110751b294e3db67aed4e594495a6 5510hi-cmw710-freeradius-r3507-US.bin 2e81e9953fe51795ee3139c8d9fad7fd3aa571b87342e7e6be10bcda4fa448be
iMC version	iMC BIMS 7.3 (E0502) iMC EAD 7.3 (E0604) iMC EIA(TAM) 7.3 (E0604P01) iMC EIA(UAM) 7.3 (E0604P01) iMC NTA 7.3 (E0506P03) iMC PLAT 7.3 (E0703) iMC QoSM 7.3 (E0504) iMC RAM 7.3 (E0502) iMC SHM 7.3 (E0506)
iNode version	iNode PC 7.3 (E0538)
Web version	None
Remarks	None

Display the system software and Boot ROM versions of 5510HI:

```
<HPE>display version
HPE Comware Software, Version 7.1.070, Release 3507    ------ Note①
Copyright (c) 2010-2021 Hewlett Packard Enterprise Development LP
HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A uptime is 0 weeks, 0 days, 2 hour
s, 43 minutes
Last reboot reason : User reboot
```

```
Boot image: flash:/5510hi-cmw710-boot-R3507-US.bin
Boot image version: 7.1.070, Release 3507
  Compiled Jun 08 2021 11:00:00
System image: flash:/5510hi-cmw710-system-R3507-US.bin
System image version: 7.1.070, Release 3507
  Compiled Jun 08 2021 11:00:00


Slot 1:
Uptime is 0 weeks,0 days,2 hours,43 minutes
5510 24G SFP 4SFP+ HI 1-slot Switch with 2 Processor
BOARD TYPE:          5510 24G SFP 4SFP+ HI 1-slot Switch
DRAM:                1984M bytes
FLASH:               512M bytes
PCB 1 Version:       VER.A
Bootrom Version:     127                ------ Note②
CPLD 1 Version:      001
CPLD 2 Version:      001
Release Version:     HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A-3507
Patch Version  :     None
Reboot Cause   :     UserReboot
[SubSlot 0] 16GE+8COMBO+4SFP Plus
```

ISSU upgrade type matrix

ISSU provides two upgrade types: compatible upgrade and incompatible upgrade. Table 3 provides the approved ISSU upgrade types only between the current version and the history versions within the past 18 months. This matrix does not include history versions that are 18 months earlier than the current version, for which, no ISSU upgrade verification is performed.

For more information about ISSU, see the fundamental configuration guide for the device.

Table 3 ISSU version compatibility matrix

Current version	History version	ISSU upgrade method
5510HI-CMW710-R3507-US	5510HI-CMW710-R3506P11	Compatible
	5510HI-CMW710-R3506P10	Compatible
	5510HI-CMW710-R3506P08	Not Support

Upgrade restrictions and guidelines

Before performing a software upgrade, it is important to refer to the *Software Feature Changes* document for any feature changes in the new version. Also check the most recent version of the related documents (see "Related documents") available on the HPE website for more information about feature configuration and commands.

Hardware feature updates

Hardware feature updates in R3507-US

None

Hardware feature updates in R3506P11

None

Hardware feature updates in R3506P10

None

Hardware feature updates in R3506P08

None

Hardware feature updates in R3506P06

None

Hardware feature updates in R3506P03

None

Hardware feature updates in R3506P02

None

Hardware feature updates in R3506P01

Added support for the SFP-XG-LH40-SM1270-BIDI, SFP-XG-LX-SM1270-BIDI, SFP-XG-LX-SM1330-BIDI, and SFP-XG-LH40-SM1330-BIDI transceiver modules.

Hardware feature updates in R3506

None

Hardware feature updates in R1311P02

None

Hardware feature updates in R1311P01

None

Hardware feature updates in R1309P07

None

Hardware feature updates in R1309P06

None

Hardware feature updates in R1309P03

None

Hardware feature updates in R1309

None

Hardware feature updates in R1308

None

Hardware feature updates in R1121P03

None

Hardware feature updates in R1121P02

None

Hardware feature updates in R1121P01

None

Hardware feature updates in R1121

- The data in **错误!未找到引用源。** was modified according to the newest test results.
- Added support for HPE X140 40G QSFP+ LC BiDi 100m MM Transceiver (JL251A).

Hardware feature updates in R1120P10

None

Hardware feature updates in R1120P07

None

Hardware feature updates in R1120

None

Hardware feature updates in R1118P02

None

Hardware feature updates in R1118

None

Hardware feature updates in R1111P01

First release

Software feature and command updates

For more information about the software feature and command update history, see *HPE 5510HI-CMW710-R3507-US Release Notes (Software Feature Changes).*

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
5510HI-CMW710-R3507-US			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R3506P11			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R3506P10			
New	savi.mib	SAVI-MIB	Added the following objects to SaviObjectsSystemEntry: saviObjectsSystemNotifySpoofing used for setting or obtaining the status of packet spoofing logging. saviObjectsSystemNotifyFilter used for setting or obtaining the status of filtering entry logging. saviObjectsSystemNotifySpoofingInterval used for setting or obtaining the log output interval for packet spoofing logging.

Item	MIB file	Module	Description
			saviObjectsSystemNotifySpoofingNumber used for setting or obtaining the maximum number of log messages that can be output per interval. saviObjectsSystemBindingCount used for obtaining the number of binding entries. saviObjectsSystemFilteringCount used for obtaining the number of filtering entries. Added the following object to SaviObjectsCountEntry: saviObjectsCountFilterOctets used for obtaining the byte count for spoofed packets filtered by SAVI.
Modified	None	None	None
5510HI-CMW710-R3506P08			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R3506P06			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R3506P03			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R3506P02			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R3506			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1311P02			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1311P01			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1309P07			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1309P06			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
5510HI-CMW710-R1309P03			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1309			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1308			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1121P03			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1121P02			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1121P01			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1121			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1120P10			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1120P07			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1120			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1118P02			
New	None	None	None
Modified	None	None	None
5510HI-CMW710-R1111P01			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R3507-US

- When the number of MAC address entries learned on a port reaches the upper limit, the message generated for this issue has changes.
  - Before modification: The message is `The number of MAC address entries exceeded the maximum number.`
  - After modification: The message is `The number of MAC address entries reached the maximum number.`

Operation changes in R3506P11

- Removed consistency check between the specified and actual airflow directions of the fan trays.
- Excluded the *freeradius.bin* file from the IPE file.

Operation changes in R3506P10

None

Operation changes in R3506P08

None

Operation changes in R3506P06

The following commands were added to the default configuration file:

```
password-control enable
#
local-user admin
service-type terminal
authorization-attribute user-role network-admin
#
user-interface aux 1
authentication-mode scheme
#
undo password-control aging enable
undo password-control composition enable
undo password-control history enable
undo password-control length enable
password-control login idle-time 0
password-control login-attempt 3 exceed unlock
password-control update-interval 0
```

Operation changes in R3506P03

None

Operation changes in R3506P02

None

Operation changes in R3506P01

None

Operation changes in R3506

After you set the speed to 100 Mbps and the duplex mode to full on an interface installed with a GE transceiver module, the interface can work with an interface with a 100MB transceiver module installed.

Modified the 802.1p priority in the VLAN tags of ARP replies sent by the device from 0 to 6

Operation changes in R1311P02

None

Operation changes in R1311P01

Providing RPS failure log messages

The device outputs the RPS Failed log message when you remove an RPS DC power cable.

Operation changes in R1309P07

None

Operation changes in R1309P06

None

Operation changes in R1309P03

- Changed the ACL issuing operation

  Before modification: For authentication users with the same authorization ACL, Layer 2 ACLs are issued based on client MAC addresses.

  After modification: For authentication users with the same authorization ACL, Layer 2 ACLs are issued based on CLASS-IDs rather than client MAC addresses. The device uses the same CLASS-ID when issuing Layer 2 ACLs to authentication users with the same authorization ACL, which saves ACL resources.

Operation changes in R1309

None

Operation changes in R1308

Before the modification: A PoE switch enabled with LLDP does not perform any operations if it has not received any LLDP frames from a connected AP before the defined timer expires.

After the modification: A PoE switch enabled with LLDP power cycles the PoE port (PI) and reboots a connected AP forcibly if it has not received any LLDP frames from the AP before the defined timer expires.

Operation changes in R1121P03

None

Operation changes in R1121P02

None

Operation changes in R1121P01

None

Operation changes in R1121

None

Operation changes in R1120P10

None

Operation changes in R1120P07

None

Operation changes in R1120

None

Operation changes in R1118P02

None

Operation changes in R1118

None

Operation changes in R1111P01

First release

Restrictions and cautions

The following transceiver modules can only work in the SFP+ ports of an HPE 5130/5510 10GbE SFP+ 2-port module (JH157A). Do not install the transceiver module in an SPF+ port on the front panel.

- HPE X130 10G SFP+ LC LRM transceiver modules (JD093B)
- HPE X130 10G SFP+ LC LH 80km Transceiver (JG915A)
- HPE X130 10G SFP+ LC ER 40km Transceiver (JG234A)

When you configure 802.1X authentication and MAC authentication, follow these restrictions:

a. When users with ACLs assigned exist on a single port, you must assign ACLs (for example, ACLs with the permit rule) to the users that do not need ACLs assigned. This operation ensures that these users do not mistakenly match ACLs of other users.

b. You must adjust the ACL rule positions to ensure that the traffic of each online user can match rules in the ACL assigned to the user.

c. When multiple users come online on a port and the same ACL is assigned to these users, to add rules to or delete rules from the ACL, you must first log off all users on the port and then add or delete ACL rules. Otherwise, some deleted ACL rules will remain.

If you configure both a PBR policy and an inbound QoS policy containing a traffic policing action, only the PBR policy takes effect on the traffic matching both policies.

If you configure both a PBR policy and a QoS policy containing a deny action, only the PBR policy takes effect on the traffic matching both policies.

Open problems and workarounds

None.

List of resolved problems

Resolved problems in R3507-US

202105110200

- Symptom: An incorrect neighbor management address is displayed in the output from the **display lldp neighbor-information verbose** command.
- Condition: This symptom occurs if the following conditions exist:

- The length of the value in the Management Address TLV is less than 8 bytes in the CDP packets received by the device.
- The total length of the Management Address TLV is less than 12 bytes.

202104220726

- Symptom: User credential information leaks.
- Condition: This symptom might occur when the user logs in to the Web interface of the device.

202105211293

- Symptom: When the SNMP NMS reads the temperature sensor MIB node, an alarm is generated abnormally.
- Condition: This symptom occurs if the device does not have an OAP security subcard inserted.

202105060531

- Symptom: Host routes become invalid on an IRF fabric after a master/subordinate switchover.
- Condition: This symptom occurs if the host routes have different next hops.

202105110235

- Symptom: The number of secure MAC addresses on a port has reached the upper limit. However, port security does not work as expected when a user moves from another port to this port.
- Condition: This symptom occurs if the following operations are performed:
  a. Port security is enabled on both of the ports. On each of the ports, the MAC address of a user is configured as a secure MAC address. The secure MAC addresses configured on the two ports are different.
  b. The two ports learn MAC addresses from each other.
  c. The users that use the configured secure MAC addresses move between the two ports.

202103290727

- Symptom: The netmeisterd process runs abnormally on an IRF fabric.
- Condition: This symptom occurs if third-party network management software cannot correctly recognize the H3C IRF fabric and issues a command to reboot the master device of the IRF fabric.

202102230116

- Symptom: The DHCP address pool fails to assign IP addresses to clients from its second secondary subnet.
- Condition: This symptom might occur if no IP addresses are available for dynamic allocation on the primary subnet and first secondary subnet in the DHCP address pool.

202104200379

- Symptom: The device reboots unexpectedly after running for a period of time.
- Condition: This symptom occurs if the device receives IP packets destined to 239.255.255.250 and with the TTL as 1 or 2.

202102150008

- Symptom: The **netconf log source all verbose** command gets stuck on an IRF fabric with an extremely low probability.
- Condition: This symptom might occur after a master/subordinate switchover if the IRF fabric is configured with loop detection and AAA or NETCONF services exist on the IRF fabric.

202103241845

- Symptom: After you modify the device IP, the device can still access the network.
- Condition: This symptom occurs if the actual number of ARP snooping entries on the device is different from that collected by the counter.

202102160026/202102221454

- Symptom: Online MAC authentication users are logged out on an IRF fabric because their idle timeout timer expires. However, the users are continuously sending traffic to the device.
- Condition: This symptom occurs if a master/subordinate switchover has occurred on the IRF fabric.

202102100037

- Symptom: A number of MAC authentication users are logged out on an IRF fabric after a master/subordinate switchover.
- Condition: This symptom occurs if the online duration of these MAC authentication users is longer than the session timeout period assigned by the server after the master/subordinate switchover.

202104200312

- Symptom: MAC authentication users cannot come online on a port.
- Condition: This symptom might occur if the MAC authentication users come online and go offline repeatedly on the port when the following conditions exist:
  - The port is enabled with both 802.1X authentication and MAC authentication.
  - The port is configured with the 802.1X guest VLAN.

Resolved problems in R3506P11

202101190167

- Symptom: After ARP fast update is enabled for MAC address moves, IPv6 ND entries are not fast updated when MAC addresses move.
- Condition: This symptom might occur after the **`mac-address mac-move fast-update`** command is executed.

202101190137

- Symptom: The device reboots automatically with a low probability when it runs the R3506P08 or R3506P10 software version. The reboot reason is reported as **UserReboot**.
- Condition: This symptom might occur when the device runs the R3506P08 or R3506P10 software version.

Resolved problems in R3506P10

202010120344

- Symptom: An IRF master device hangs and cannot be accessed through the console port.
- Condition: This symptom might occur if an IRF fabric receives packets shorter than 64 bytes.

202008260498

- Symptom: Port isolation does not take effect on an aggregate interface.
- Condition: This symptom might occur if port isolation is configured on an aggregate interface where multiple ACs exist.

202007300268

- Symptom: An aggregate interface where ACs are configured for MPLS L2VPN fails to forward some packets.
- Condition: This symptom might occur if ACs are configured for MPLS L2VPN on an aggregate interface.

202009220628

- Symptom: The device cannot identify phone offline events.
- Condition: This symptom might occur if the device is attached to phones that do not send CDP packets periodically, such as Polycom and AudioCodes phones.

202009280287

- Symptom: CVE-2020-10188
- Condition: utility.c in telnetd in netkit telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.

202008240782

- Symptom: The Telnet process hangs.
- Condition: This symptom might occur if command accounting is enabled and the AAA server is unreachable.

202008240177

- Symptom: Users fail their first portal authentication attempts while passing the second one.
- Condition: This symptom might occur if both the **portal apply mac-trigger-server** and **portal apply web-server settings are** configured.

Resolved problems in R3506P08

202007271063

- Symptom: The device might fail to start properly with a very low probability.
- Condition: This symptom occurs if the device is repeatedly power-cycled.

Resolved problems in R3506P06

202005271313

- Symptom: 1-Gbps fiber ports do not come up.
- Condition: This symptom occurs because 1-Gbps fiber ports cannot be connected to SGMII devices.

202005291034

- Symptom: An aggregate interface does not load share TCP or UDP traffic among member links.
- Condition: This symptom might occur if TCP or UDP traffic is forwarded out of an aggregate interface.

202004020936

- Symptom: Clock synchronization fails after an ISSU is performed.
- Condition: This symptom occurs if you use **the ntp-service source** command to specify a source interface for NTP messages before performing the ISSU.

202005111273

- Symptom: The combo ports on all IRF subordinate devices go down after a master/subordinate switchover.
- Condition: This symptom occurs if the master/subordinate switchover occurs after the original master device reboots or the entire IRF fabric reboots.

Resolved problems in R3506P03

202002170517

- Symptom: Multiple Ethernet service instances are configured on a port. The frame match criterion of only one Ethernet service instance takes effect.
- Condition: This symptom occurs if the encapsulation default command is executed for an Ethernet service instance on the port.

202001170358

- Symptom: 802.1X users and MAC authentication users come online through the same port. The ACL issued to users that come online later does not take effect.
- Condition: This symptom occurs if the following operations have been performed:
  a. Configure both MAC authentication and 802.1X authentication on a port.
  b. Issue the same ACL to users.

Resolved problems in R3506P02

201912170108

- Symptom: When the PoED process is restarted, the process does not respond.
- Condition: This symptom occurs if the following conditions exist:
  - Multiple PoE-capable devices form an IRF fabric.
  - The master and subordinate member devices all act as PSEs to supply power.
  - The PoED process is restarted every 20 seconds.

201911070588

- Symptom: The SSHD call stack might be printed.
- Condition: This symptom occurs if you log in to the device repeatedly through SSH.

201908270157

- Symptom: After a user passes 802.1X authentication and enters the username and password on a PC, ErrCode=0 appears on the switch and the user goes offline. About half a minute to one minute later, the user performs authentication again and comes online.
- Condition: This symptom occurs if the following operations are performed:
  - On an interface configured with port-based access control, configure the guest VLAN and the hybrid port is removed from the default VLAN (VLAN 1).
  - After a user passes 802.1X authentication, the user modifies the username and password and initiates authentication again.

Resolved problems in R3506P01

201909250124

- Symptom: Some interfaces on the device go down.
- Condition: This symptom occurs if the copper ports of the device are configured to autonegotiate their speeds and are connected to APs.

201908270091

- Symptom: After an IRF physical interface is switched to a common interface, multicast traffic is forwarded abnormally on the interface.

- Condition: This symptom occurs if an IRF physical interface is switched to a common interface after IP multicast forwarding is enabled.

Resolved problems in R3506

201904220057

- Symptom: The device tries to obtain the manufacturing information of a fan tray repeatedly, resulting in memory leak.
- Condition: This symptom occurs when no manufacturing information is coded into the fan tray.

201906200052

- Symptom: The port security, LLDP, and interface management processes become deadlocked.
- Condition: This symptom occurs with a low probability if port security is configured on the device and an intrusion protection is triggered.

201906110727

- Symptom: Each time the device is automatically configured after startup, the IP address that it obtains through DHCP is different from the most recent one.
- Condition: This symptom might occur if the configuration on the device is deleted before it reboots and the device is automatically configured after startup.

201906050407

- Symptom: When many-to-one VLAN mapping is configured on the device, a connected terminal cannot ping the extranet after it re-obtains an IP address.
- Condition: This symptom might occur if the terminal re-obtains the IP address after the port through which the terminal connects to the device is moved from an original VLAN to the translated VLAN.

201904200142

- Symptom: On an MPLS L3VPN network, the next hop of the route to the public tunnel is unreachable.
- Condition: This symptom might occur if the device acts as a PE device and the next hop of the route to the public tunnel is equal cost routes but load sharing is not used.

201904160395

- Symptom: The device fails to learn MAC address entries.
- Condition: This symptom might occur if the device has already learned a large number of MAC address entries and multiple ports keep flapping.

201904150324

- Symptom: When the device is configured to display log buffer information and buffered logs, it displays only the newest log rather than all logs in the log buffer.
- Condition: This symptom might occur if the display operation is repeatedly performed after the log buffer gets full.

201904101024

- Symptom: An IRF fabric is split unexpectedly and it cannot process protocol packets correctly.
- Condition: This symptom might occur if an IRF physical interface or a 10-GE port that resides on the same interface module as the IRF physical interface receives a packet with less than 64 bytes.

201904100097

- Symptom: CFD loopback does not take effect on a service instance.
- Condition: This symptom might occur if the MAs in the service instance are configured without carrying the VLAN attribute.

201903290697

- Symptom: Traffic on the main interface of a Layer 3 Ethernet subinterface cannot be forwarded correctly after the subinterface is shut down.
- Condition: This symptom might occur if the Layer 3 Ethernet subinterface is shut down by using the **shutdown** command.

201903280212

- Symptom: Traffic on Layer 3 aggregate subinterfaces in an IRF fabric cannot be forwarded correctly after the IRF fabric reboots.
- Condition: This symptom might occur if the running configuration is saved and the IRF fabric is rebooted after Layer 3 aggregate subinterfaces are configured.

201902020370

- Symptom: Only eight ports on the PoE-capable device can supply power.
- Condition: This symptom might occur if an exception exists on the power management configuration register.

201905140328

- Symptom: When port security is configured, traffic forwarding fails because of secure MAC address loss after the entire IRF fabric reboots or a member device that has secure MAC addresses reboots.
- Conditions: This symptom might occur if the IRF fabric contains three or more member devices and the entire IRF fabric reboots or a member device that has secure MAC addresses reboots.

201605180448

- Symptom: On a PE, the **display l2vpn mac-address** command cannot display the MAC address entries for VSIs.
- Condition: This symptom occurs if VPLS is configured through LDP and the switch can forward packets properly.

Resolved problems in R1311P02

201901210259

- Symptom: The PBR feature does not take effect.
- Condition: This symptom occurs if PBR is configured on a Layer 3 aggregate interface.

Resolved problems in R1311P01

201812060189

- Symptom: A user cannot log in to the switch through SSH when the number of online SSH users reaches 32.
- Condition: This symptom occurs if the device does not update the number of online SSH users after the SSH client logs out.

201812060193

- Symptom: The xmlcfgd process exits unexpectedly and a core file is created.
- Condition: This symptom occurs if the following operations have been performed:
  a. Bind more than 13 static addresses to the DHCP address pool.
  b. Use the SoapUI tool to perform a GET operation on the DHCP/DHCPServerPoolStatic table.

201812060181

- Symptom: The switch reboots unexpectedly after IPsec is configured.
- Condition: This symptom occurs if IPsec is configured.

201812060220

- Symptom: A packet is discarded because it is incorrectly determined as an MPLS ping packet.
- Condition: This symptom occurs if the packet is a UDP fragment and the content after the IP header is the same as the UDP port number (3053).

201811130200

- Symptom: The port security process is locked.
- Condition: This symptom occurs if the following conditions exist:
  - The intrusion protection mode is disableport-temporarily on a port.
  - Port security triggers intrusion protection and sets the port to the down state while LLDP is obtaining user data from port security.

201811050088

- Symptom: The device is connected to an IMC server for portal authentication. The device is logged out because of security check failures.
- Condition: This symptom occurs if the device is connected to an IMC server and IMC is configured with a security policy to perform security check for the device.

201811140403

- Symptom: CVE-2018-15473
- Condition: OpenSSH is prone to a user-enumeration vulnerability. An attacker may leverage this issue to harvest valid user accounts, which may aid in brute-force attacks. OpenSSH through 7.7 are vulnerable; other versions may also be affected.

201811300199

- Symptom: A portal user fails re-DHCP authentication, with a "Nonexistent username" error message prompted.
- Condition: This symptom might occur when a portal user performs re-DHCP authentication.

201811050128

- Symptom: Memory leaks occur to the service using the fast forwarding table.
- Condition: This symptom occurs if the following conditions exist:
  a. A large amount of traffic with varying quintuples is sent to the CPU through fast forwarding.
  b. The fast forwarding entries age out.

201811050119

- Symptom: Two devices use IKEv2 negotiation to set up IPsec SAs, and use the security protocol ESP. After TFC padding is enabled, the length of the padded packets exceeds the MTU of the local interface. As a result, packets are dropped.
- Condition: This symptom occurs if the following conditions exist:

a. The **tfc enable** command is used to enable TFC padding on the peer device.
b. The length of the padded packets (the original packet length + the TFC padding length) exceeds the MTU of the local interface. Packet fragmentation is disabled.

201811050107

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs if the VPN instance and IP address configuration of a 40-GE interface are modified when the interface is sending or receiving packets.

201810230544

- Symptom: The RADIUS server fails to authorize a VLAN name to a user.
- Condition: This symptom occurs if the RADIUS server authorizes a VLAN name in the format of \000XXXXX\000 to a user passing AAA authentication.

201810230551

- Symptom: The memory of the standby MPU leaks.
- Condition: This symptom occurs if a portal client comes online carrying the option82 (v4) or option18 (v6) information on an IRF fabric.

201811010430

- Symptom: The **dot1x offline-detect** and **dot1x offline-detect enable** commands executed on the device do not take effect.
- Condition: This symptom occurs if the software of the device is upgraded to the current version by using ISSU.

201810180032

- Symptom: When you enable BFD on an aggregate interface, the system prompts that the operation failed.
- Condition: This symptom occurs if the low bits of the source IP address and destination IP address are multicast addresses when you enable BFD on an aggregate interface.

201809050571

- Symptom: The controller issues the save command to the switch every 30 minutes and is disconnected from the switch immediately after the command is issued. When the display process command is executed, the output shows that a large number of residual configuration copy processes exist on the switch.
- Condition: This symptom might occur if the controller issues the save command to the switch every 30 minutes and is disconnected from the switch immediately after the command is issued.

201809050485

- Symptom: The peer sends IS-IS LSPs with the overload bit set to the switch. When the next hop for reaching the peer changes, the switch calculates a wrong outgoing interface for the traffic to be sent to the peer.
- Condition: This symptom might occur if the peer sends IS-IS LSPs with the overload bit set to the switch and the next hop for reaching the peer changes.

201807160277

- Symptom: When the RPS is installed, the RPS LED is not on, and the display power command does not display the RPS status.
- Condition: This symptom might occur if the RPS is installed.

201810120342

- Symptom: The switch cannot obtain the incoming and outgoing port numbers for traffic on an sFlow-enabled interface.
- Condition: This symptom might occur if sFlow is enabled on an interface.

201810150077

- Symptom: After a two-chassis IRF fabric reboots, MAC authentication users fail authentication on a port of the subordinate member.
- Condition: This symptom might occur if the IRF member devices each have a port that is working in the **userlogin-secure-or-mac** port security mode and MAC authentication users perform authentication on the port on the subordinate member after the IRF fabric reboots.

201809140102

- Symptom: Port security configuration changes after a software upgrade.
- Condition: This symptom might occur if the port security-configured switch is upgraded to R1309P06 or R1309P07.

201812110031

- Symptom: A host is directly connected to the management Ethernet interface of an IRF member device. After an IRF master/subordinate switchover, the host cannot ping the management Ethernet interface.
- Condition: This symptom might occur if the IRF fabric splits and the IRF member device that owns the IRF bridge MAC address fails to re-join the IRF fabric before the IRF bridge MAC persistence timer expires.

Resolved problems in R1309P07

201808290664

- Symptom: In the **display dot1x** command output, the **Offline detect period** field is not aligned with the other fields.
- Condition: This symptom occurs if the **display dot1x** command is executed.

201809050749

- Symptom: Some deleted MAC address entries might remain.
- Condition: This symptom occurs if a large number of MAC address entries are learned and the **undo mac-address** command is used to delete MAC address entries.

201808170356

- Symptom: Mirrored packets are encapsulated with GRE headers when GRE tunnels are not configured.
- Condition: This symptom occurs if flow mirroring is configured.

201808160104

- Symptom: The MIB-Browser fails to read information of the DHCP server MIB nodes.
- Condition: This symptom occurs if the MIB-Browser is used to read information of the DHCP server MIB nodes.

201809050679

- Symptom: The local mirroring configuration does not take effect after the device is rebooted.
- Condition: This symptom occurs if STP is configured globally, local mirroring is configured, and then the device is rebooted.

201808200338

- Symptom: BGP neighbor relationship cannot be established between the specified two link-local addresses.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure link-local addresses for both the local interface and peer interface.
  b. Use the **peer** command to establish BGP neighbor relationship between the two link-local addresses.

201712080156

- Symptom: The LDP process exits exceptionally.
- Condition: This symptom occurs if the following conditions exist:
  a. A PC is directly connected to the device.
  b. MPLS LDP is configured on the device.
  c. The PC continuously sends LDP Label Mapping messages.

201807190555

- Symptom: The NMS memory leaks.
- Condition: This symptom occurs if the **undo snmp-agent trap enable** command is used to disable SNMP notifications and the NMS walks on the SYSLOG-MSG-MIB node information.

201808020501

- Symptom: The device fails to obtain the authorization VLAN name in the \000xxxxx\000 format from the RADIUS server.
- Condition: This symptom might occur if the RADIUS server issues an authorization VLAN name in the \000xxxxx\000 format to an authenticated user.

201807310087

- Symptom: HTTPS redirection fails.
- Condition: This symptom occurs if HTTPS redirection is enabled and a user uses the browser in the MAC OS to access the server.

201806050164

- Symptom: The configuration of a Layer 3 aggregate interface is lost.
- Condition: This symptom occurs if a Layer 3 aggregate interface is configured, the configuration is saved, and the device is rebooted.

201808140119

- Symptom: The ACL function does not take effect.
- Condition: This symptom occurs if 802.1X issues authorization ACLs.

201808070167

- Symptom: A user that fails to pass MAC authentication cannot perform Web authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. An interface is configured with both MAC authentication and Web authentication.
  b. A user fails to pass MAC authentication.

201808060785

- Symptom: An 802.1X authentication server fails to issue authorization ACLs.
- Condition: This symptom occurs if 802.1X authentication is enabled and the authentication server issues authorization ACLs containing rules related to TCP or UDP services and port numbers to users.

201807210046

- Symptom: After a user logs in to the device by using SSH and then goes offline, remaining information of the user exists on the device.
- Condition: This symptom occurs if the user logs in to the device and then goes offline by using SSH frequently.

201807120164

- Symptom: Some UDP packets with the destination port number 6784 are lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure BFD MAD on an IRF fabric.
  b. The IRF fabric receives UDP packets with the destination port number 6784.

Resolved problems in R1309P06

201804260662

- Symptom: The following problems occur:
  - When a user performs authentication through HWTACACS, the user cannot successfully log in, and no debugging information is printed.
  - When a user performs authentication through RADIUS, the user can successfully log in, but part of the debugging information is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Configure the AAA authentication method as HWTACACS or RADIUS.
  b. A user logs in to the device through Telnet, enters an incorrect password, and then immediately enters the correct password to log in.

201806290399

- Symptom: The value of the snmpEngineboot node is incorrect.
- Condition: This symptom occurs if the whole IRF fabric is rebooted to cause a master/subordinate switchover.

201807040644

- Symptom: PBR does not take effect on ports in a super VLAN.
- Condition: This symptom occurs if PBR is configured on a super VLAN interface.

201712020228

- Symptom: The entPhysicalDescr node value cannot be obtained for the second interface on a 40-G subcard.
- Condition: This symptom occurs if a MIB tool is used to read the value of the entPhysicalDescr node.

201807040637

- Symptom: When the spanning tree protocol is disabled globally, spanning tree protocol packets cannot be flooded.
- Condition: This symptom occurs if the spanning tree protocol is disabled globally.

201807040593

- Symptom: After you modify the login password on the Web interface, you will fail to log in to the device again. In this case, you must set the password again.
- Condition: This symptom occurs if you log in to the device through the Web interface and modify the login password.

201806080831

- Symptom: When a master/subordinate switchover occurs on an IRF fabric, the subordinate member device cannot properly establish the TCP three-way handshake with the peer device. As a result, BGP might flap.
- Condition: This symptom occurs if the IRF fabric has NSR enabled or the subordinate member device is rebooted.

201806080845

- Symptom: In the rd1 table, routes with the same prefix as routes of rd2 are all deleted.
- Condition: This symptom occurs if the following operations are performed:
  a. When VPNv4 routes of rd1 and rd2 are advertised to the peer device, the peer device matches and accepts only VPNv4 routes of rd1.
  b. Withdrawal messages for VPNv4 routes of rd1 and rd2 are advertised to the peer device.
  c. When receiving the withdrawal messages for VPNv4 routes of rd2, the peer device selects VPNv4 routes with the same prefix as VPNv4 routes of rd2 in the rd1 table and deletes these routes.

201806110066

- Symptom: The outgoing interface is incorrectly calculated for an IS-IS route.
- Condition: This symptom occurs if the MAC address of the peer device changes after the peer device establishes the IS-IS neighbor relationship with the local device.

201805250708

- Symptom: CVE-2016-9586
- Condition: Attackers can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

201804260567

- Symptom: NMS receives traps more than 10 minutes after the device reboots.
- Condition: This symptom occurs if the security model of SNMPv3 is authentication with privacy and the SNMP agent device is rebooted.

201804260682

- Symptom: ISSU upgrade fails.
- Condition: This symptom occurs if ISSU is used to upgrade the software when the **packet-filter** configuration exists.

201806110087

- Symptom: The device might not respond when the **display ike sa** command is executed.
- Condition: This symptom occurs if the device acts as the IKE responder, and IKE SAs are established again after old IKE SAs are aged and deleted.

201806080844

- Symptom: IPsec negotiation fails.
- Condition: This symptom occurs if the VPN instance of the interface bound to an IPsec policy is different from the VPN instance of the IPsec protection process after NAT translation.

201804260604

- Symptom: IPsec tunnels are interrupted irregularly.
- Condition: This symptom occurs if IPsec are configured on two devices and the two devices initiate negotiation packets to each other at the same time.

201711290750

- Symptom: The SNMP function fails.
- Condition: This symptom occurs if the **snmp-agent port** command is used to modify the UDP port for receiving SNMP packets.

201806050863

- Symptom: The command execution result is not displayed.
- Condition: This symptom occurs if you enter the Python shell and execute Comware V7 commands.

201805290211

- Symptom: An access device cannot ping the core device.
- Condition: This symptom occurs if the following operations are performed:
  a. Two devices form an IRF fabric. The IRF fabric is connected to the core device through a multichassis aggregate link.
  b. The access device connects to the IRF fabric through an aggregate interface, and the aggregate interface is assigned to a port isolation group.
  c. Reboot the IRF fabric.

201806140516

- Symptom: ARP replies are dropped.
- Condition: This symptom occurs if a trunk port of the device sends ARP replies shorter than 64 bytes.

201806200110

- Symptom: The system does not automatically modify the QoS priorities for traffic in a voice VLAN.
- Condition: This symptom occurs if an interface has voice VLAN enabled and receives voice traffic.

201805250467

- Symptom: An interface on the device leaves the voice VLAN and cannot join the voice VLAN again.
- Condition: This symptom occurs if the following operations are performed:
  a. In an IRF fabric, an interface on a subordinate member device has LLDP enabled and voice VLAN configured, and is connected to a LLDP/CDP-capable voice device.
  b. Establish or disconnect LLDP neighbor relationship on the subordinate member device.

201805220359

- Symptom: The device continuously sends ARP requests.
- Condition: This symptom occurs if the following operations are performed:
  a. The device is configured with multiport ARP entries.
  b. Outgoing interface consistency check for ARP entries and MAC address entries is enabled.

201805250699

- Symptom: A device port learns the source MAC address in LLDP packets.
- Condition: This symptom occurs if the device port receives LLDP packets.

201806050085

- Symptom: When an LSWM5SP8PM interface card is plugged or unplugged, the interface card name is displayed as LSWM4SP8PM in the device logs.

- Condition: This symptom occurs if an LSWM5SP8PM interface card is plugged or unplugged.

201802010506

- Symptom: An IP address cannot be configured for the device.
- Condition: This symptom occurs if an IRF member device is powered off and rebooted multiple times to perform master/subordinate switchovers.

201804090636

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the following conditions exist:
  a. The network has a large number of short TCP connections.
  b. The device keeps receiving and sending packets.
  c. The device accesses resources that have been released by itself.

201804090093

- Symptom: The device reboots unexpectedly.
- Condition: This symptom might occur if the following conditions exist:
  a. A NAT server mapping is configured on an interface. In the mapping, the private IP address of the internal server is the IP address of the interface.
  b. Security control policies are frequently created and deleted when L2TP users access the internal server through the public IP address mapped to the private IP address.

201802010690

- Symptom: The device discards packets with a checksum of 01 00.
- Condition: This symptom might occur if the checksum of incoming packets is 01 00.

201711160780

- Symptom: The energy saving configuration on a combo interface gets lost after the active port of the combo interface changes from the copper port to the fiber port and then back to the copper port.
- Condition: This symptom might occur if the following operations are performed:
  a. When the copper port of the combo interface is active, enable EEE and auto power-down on the combo interface.
  b. Activate the fiber port of the combo interface.
  c. When the fiber port of the combo interface is active, activate the copper port of the combo interface.

201805090571

- Symptom: When dropping unknown multicast data packets is enabled for a VLAN, the device floods multicast packets with TTL 0 in the VLAN.
- Condition: This symptom might occur if dropping unknown multicast data packets is enabled for the VLAN.

201804270451

- Symptom: An interface sends incoming ARP requests back to the source interfaces.
- Condition: This symptom might occur after the following operations are performed:
  a. Configure the interface as an ARP trusted interface by using the arp detection trust command.
  b. Assign the interface to an aggregation group.
  c. Delete the aggregation group or remove the interface from the aggregation group.

201804240510

- Symptom: In an IRF fabric, the displayed MTU value of a Layer 2 aggregate interface on a subordinate device is incorrect.
- Condition: This symptom might occur if the following operations are performed:
  a. Configure the Layer 2 aggregate interface to allow jumbo frames within a specific length to pass through by using the jumboframe enable command.
  b. Save the running configuration and reboot the IRF fabric.

201804180241

- Symptom: The outgoing interface information is inconsistent in the MAC address entry and the ARP entry for the same MAC address.
- Condition: This symptom might occur if the MAC address moves frequently.

201805180576

- Symptom: Symptom: Non-first fragments of an IP packet, which do not contain TCP or UDP port numbers, match an ACL rule specified with TCP or UDP port numbers.
- Condition: This symptom might occur if the ACL rule is specified with TCP or UDP port numbers.

Resolved problems in R1309P03

201801190229

- Symptom: CVE-2017-15896
- Condition: An attacker can exploit this issue to bypass TLS validate and encrypt, send application data to Node.js.

201801190229

- Symptom: CVE-2017-3737
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201801190229

- Symptom: CVE-2017-3738
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201705310258

- Symptom: The device reboots exceptionally at a very low probability.
- Condition: This symptom occurs if the device has been running for a long period of time and invalid memory is accessed when PBR determines whether the next hop is valid through querying the FIB table.

201706300315

- Symptom: When the status of a track entry associated with a static route changes, the static route does not respond to the change, and status of the static route's next hop does not change.
- Condition: This symptom occurs if a static route fails to establish a connection to the track module when the static route is associated with a track entry.

201804090334

- Symptom: It takes 20 seconds to log in to the device through SSH.

- Condition: This symptom occurs if you log in to the device through SSH after the password control feature is enabled.

201705310354

- Symptom: The rawip socket remains, which exhausts the memory and causes the device to reboot.
- Condition: This symptom occurs if you keep performing NQA operation for a period of time.

201802010709

- Symptom: After the **port link-mode route** command is executed on an interface, the command does not take effect.
- Condition: This symptom occurs if the following operations are performed on an IRF fabric:
  a. Disconnect the standby MPU and LPUs of the device in sequence
  b. Restore the connections of the LPUs and standby MPU in sequence.

201706300478

- Symptom: The device cannot send ICMP error packets.
- Condition: This symptom occurs if the following conditions exist:
  - The **ip unreachables enable** and **ip ttl-expires enable** commands are configured on the device.
  - The device receives ICMP request packets.

201801290865

- Symptom: The prefix obtained from an IPv6 address is still advertised in RA messages.
- Condition: This symptom occurs if an IPv6 address is manually configured and then the **ipv6 nd ra prefix default no-advertise** command is configured to disable the device from advertising the prefix of the IPv6 address.

201802070015

- Symptom: The PoE function of interfaces still supplies power.
- Condition: This symptom occurs if PoE is disabled on all interfaces and then PoE is disabled on the PSE.

201801300024

- Symptom: Some BSR packets are dropped in a VLAN with IGMP snooping enabled.
- Condition: This symptom occurs if IGMP snooping is enabled for a VLAN and BSR packets are received at wire speed in the VLAN.

201803260509

- Symptom: The **bpdu-drop any** command configuration does not take effect.
- Condition: This symptom occurs if the following operations are performed:
  a. On an IRF fabric, configure BFD MAD. Execute the bpdu-drop any command on the IRF physical interfaces.
  b. In system view, execute the undo stp global enable/stp global enable or reboot command. The STP status of interfaces changes.

201803160619

- Symptom: With MAC authentication enabled, the device does not disconnect a user and still displays the user as online when the device does not receive any packets from the user within the offline detection timer but the MAC address entry has not aged out.
- Condition: This symptom occurs if MAC authentication offline detection is enabled and the offline detection timer is different from the MAC address aging timer.

201803200427

- Symptom: Traps are received more than 10 minutes after the device is rebooted.
- Condition: This symptom occurs if the device is rebooted when authentication with privacy is configured for SNMPv3.

201802010956

- Symptom: The connection between an IRF fabric and a controller flaps.
- Condition: This symptom occurs if the following conditions exist:
  - OpenFlow devices form an IRF fabric.
  - A subordinate member device connects to the controller.
  - The subordinate member device receives 150-byte PIM packets at wire speed.

201801300586

- Symptom: An OpenFlow device is disconnected from the controller.
- Condition: This symptom occurs if the controller issues the **openflow shutdown** or **undo openflow shutdown** command twice.

201803230514

- Symptom: After a device configured with port security is rebooted, users fail to come online through MAC authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable port security, and set the port security mode to macAddressWithRadius, macAddressOrUserLoginSecure, macAddressElseUserLoginSecure, macAddressOrUserLoginSecureExt, or macAddressElseUserLoginSecureExt on an interface.
  b. Save the configuration, and delete the .mdb configuration file.
  c. Reboot the device.

201708150559

- Symptom: Dynamic MAC-based VLAN assignment is enabled on an interface, and the PVID of the interface is a secondary VLAN of a primary VLAN. If an incoming frame is tagged with the PVID and fuzzy MAC-to-VLAN entry match succeeds for the frame's source MAC address, the interface cannot forward the frame.
- Condition: This symptom might occur if the interface receives a frame that carries a VLAN ID same as the PVID of the interface, and the PVID is a secondary VLAN of a primary VLAN.

201712220061

- Symptom: CVE-2017-3736
- Condition: An attacker can exploit this issue to gain access to sensitive information that may aid in further attacks.

201712190289

- Symptom: CVE-2017-12190
- Condition: Local attacker can exploit these issues to obtain sensitive information that may lead to further attacks.

201712190289

- Symptom: CVE-2017-12192
- Condition: Attackers can exploit this issue to cause denial-of-service conditions. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.

201712190289

- Symptom: CVE-2017-15274
- Condition: An attacker can exploit this issue to cause a local denial-of-service condition.

201712190289

- Symptom: CVE-2017-15299
- Condition: An attacker can exploit this issue to trigger a kernel panic, denying service to legitimate users.

201801190481

- Symptom: On an OpenFlow-enabled IRF fabric that contains two member switches, the **openflow shutdown** command is executed on an interface of the subordinate switch, and then the interface is brought up from the controller. After a master/subordinate switchover, status of an interface is abnormal on the new master.
- Condition: This symptom might occur if a master/subordinate switchover occurs after an interface that has been shut down by OpenFlow on the subordinate switch is brought up from the controller.

201801190469

- Symptom: On the OpenFlow-enabled switch, execution of the **openflow shutdown** command fails on an aggregate interface.
- Condition: This symptom might occur if the **openflow shutdown** command is executed on an aggregate interface.

201801180979

- Symptom: When receiving PIM bootstrap messages with a length of 1500 bytes, the switch can send only five bootstrap messages per second in a VLAN enabled with IGMP snooping.
- Condition: This symptom might occur if IGMP snooping is enabled for a VLAN.

201712230037

- Symptom: When the management Ethernet interface receives a Layer 3 packet that is not destined for the MAC address of the interface, the switch forwards the packet by using an incorrect route.
- Condition: This symptom might occur if the management Ethernet interface receives a Layer 3 packet that is not destined for the MAC address of the interface.

201801040748

- Symptom: ACLs are not completely deleted from the hardware after IP source guard configuration is deleted from a port and the VLAN interface of the VLAN to which the port is assigned.
- Condition: This symptom might occur if IP source guard configuration is deleted from a port and the VLAN interface of the VLAN to which the port is assigned.

201801090588

- Symptom: After a QSFP+ module or cable is removed and re-installed, the switch cannot obtain electronic label information for the module or cable or obtains incorrect information.
- Condition: This symptom might occur if a QSFP+ module or cable is removed and re-installed.

201801180968

- Symptom: The switch is connected to a VRRP group. After the link between the VRRP master and the switch flaps, the switch has an incorrect ARP entry for the VRRP master.
- Condition: This symptom might occur if the switch is connected to a VRRP group, and the link between the VRRP master and the switch flaps.

201711290635

- Symptom: When a port joins a Layer 2 aggregation group, the allowed jumbo frame length configured on the Layer 2 aggregate interface is not synchronized to that port.
- Condition: This symptom might occur if a port joins a Layer 2 aggregation group that is configured with the allowed jumbo frame length setting.

201712210545

- Symptom: In the output from the **display transceiver diagnosis interface** command, the receive power of transceiver modules is incorrect.
- Condition: This symptom might occur if the **display transceiver diagnosis interface** command is executed.

201711290741

- Symptom: On a MPLS network, the LDP process on the device exits unexpectedly after receiving specific LDP messages from a device of the other vendors.
- Condition: This symptom might occur if the device acts as a PE device and establishes a connection with a device of the other vendors.

201711030370

- Symptom: CVE-2017-1000253
- Condition: Local attackers may exploit this issue to gain root privileges.

201711230489

- Symptom: The device reboots unexpectedly when reading an Entity MIB node.
- Condition: This symptom might occur if the device reads an Entity MIB node.

201711230366

- Symptom: The device reboots unexpectedly after receiving a packet-out message without the output or group action issued by the controller.
- Condition: This symptom might occur if the device receives a packet-out message without the output or group action issued by the controller.

201711250324

- Symptom: Two devices are connected through interfaces on the LSWM2XGT8PM expansion modules. When the interface of a device is enabled with external loopback testing, the interface cannot come up and the peer interface on the other device flaps.
- Condition: This symptom might occur if the two devices are connected through interfaces on the LSWM2XGT8PM expansion modules and the interface on a device is enabled with external loopback testing.

201711230694

- Symptom: The device might fail to delete the configurations of HWTACACS servers when the configurations of HWTACACS servers are frequently deleted. Or, a process exception might occur if the device rolls back the configuration.
- Condition: This symptom might occur if the following conditions exist:
  - The HWTACACS scheme configured on the device contains configurations of multiple HWTACACS authentication, authorization, and accounting servers.
  - The HWTACACS authentication, authorization, or accounting servers have the same VPN instance and IP address settings but different port numbers.

201710100183

- Symptom: When receiving unknown Layer 2 unicast packets of a VLAN, the device floods the packets on all Layer 3 Ethernet subinterfaces and Layer 3 aggregate subinterfaces of which the subinterface number is the same as the VLAN ID.
- Condition: This symptom might occur if Layer 3 Ethernet interfaces or Layer 3 aggregate interfaces have a subinterface of which the subinterface number is the same as the VLAN ID of incoming unknown Layer 2 unicast packets.

201712040081

- Symptom: In an IRF fabric, the console port on the subordinate device hangs and some information of the subordinate device cannot be viewed on the master device.
- Condition: This symptom might occur if the following conditions exist:
  - The IRF fabric is configured with the spanning tree feature.
  - The peer switch is disabled with the spanning tree feature.
  - A loop exists between the IRF fabric and the peer switch.

201711280600

- Symptom: After certain operations are performed, the **display mac-address** command does not display the voice VLAN MAC address entry of an IP phone. When the settings on the interface connected to the IP phone are removed and reconfigured, the IP phone cannot join a voice VLAN.
- Condition: This symptom might occur if the following operations are performed:
  a. Connect an IP phone to an interface.
  b. Configure voice VLAN and port security on the interface.
  c. Remove the settings from the interface and reconfigure them on the interface.

201711280538

- Symptom: MAC address entries of MAC authentication users do not age out after the users go offline.
- Condition: This symptom might occur if the following conditions exist:
  - A Layer 2 switch configured with the spanning tree feature exists between the device and the authentication clients.
  - The device is enabled with MAC authentication.
  - The aging timer for dynamic MAC address entries is set to a value greater than 60 seconds by using the **mac-address timer aging** *seconds* command.

201710300395

- Symptom: A remark action conflict is prompted when a QoS policy containing both an 802.1p priority marking action and a local precedence marking action in the same behavior is applied.
- Condition: This symptom might occur if a QoS policy containing both an 802.1p priority marking action and a local precedence marking action in the same behavior is applied.

201711110038

- Symptom: A user fails 802.1X or MAC authentication when the VLAN tag setting of the server-assigned authorization VLAN is different from that of the VLAN where the user resides
- Condition: This symptom might occur if the VLAN tag setting of the server-assigned authorization VLAN is different from that of the VLAN where the user resides.

201709250409

- Symptom: The mirroring and STP settings are partially lost.

- Condition: This symptom occurs if the following operations are performed:
  a. Delete some SNMP settings.
  b. Save the configuration by using the save force command and reboot the device.

201708280341

- Symptom: MAC authentication fails after certain operations are performed.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security, and set the port security mode to userlogin-secure-or-mac on an interface.
  b. Save the configuration and upgrade the software, or reboot the switch and use a .cfg file to restore the configuration.

201708280275

- Symptom: An 802.1X user that passes authentication on an interface is assigned an IP address in the guest VLAN, Auth-Fail VLAN, or critical VLAN instead of an IP address in the authorization VLAN.
- Condition: This symptom might occur if the following conditions exist:
  - Both 802.1X and DHCP are enabled.
  - An 802.1X guest VLAN, Auth-Fail VLAN, or critical VLAN is configured on the interface.
  - The server successfully assigns an authorization VLAN.

201708280259

- Symptom: 802.1X authentication fails on an interface.
- Condition: This symptom might occur if the following operations are performed:
  - Enable 802.1X and specify the port-based access control method on an interface.
  - Set the username request timeout timer by using the **dot1x timer tx-period** *tx-period-value* command.

201708280255

- Symptom: A user logs in to the CLI through a console port. The CLI hangs up after the user executes the **stp edged-port** and **stp loop-protection** commands in interface range view.
- Condition: This symptom might occur if AAA authentication is enabled for CLI login by using the **authentication-mode scheme** command and command accounting is enabled by using the **command accounting** command.

201709250610

- Symptom: In an IRF fabric, the **undo jumbo enable** command configuration loses effect after an ISSU is performed.
- Condition: This symptom occurs after an ISSU is performed.

201710300047

- Symptom: The **snmp-agent target-host trap** command configuration is lost after a master/subordinate switchover is performed in an IRF fabric.
- Condition: This symptom occurs if the *vpn-instance-name* or *security-string* argument in the command contains dots (.).

201708280230

- Symptom: A user passes MAC authentication on an interface with port security configured after failing 802.1X authentication. The user fails MAC authentication after the **shutdown** and **undo shutdown** commands are executed on the interface.

- Condition: This symptom occurs if the port security mode is set to **userlogin-secure-or-mac-ext** on the interface.

201710260388

- Symptom: The device does not support the ACL deployed by the 802.1X authentication server.
- Condition: This symptom occurs when a client performs 802.1X authentication.

201709250739

- Symptom: CVE-2017-3735
- Condition: Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions; this may aid in launching further attacks.

201710200010

- Symptom: Automatic configuration fails because a VLAN interface cannot obtain an IP address.
- Condition: This symptom occurs when the device starts up without a configuration file.

201709220068

- Symptom: The interface view is unavailable on an IRF member device after a master/subordinate switchover.
- Condition: This symptom occurs if new member devices are added during the master/subordinate switchover.

201708310208

- Symptom: Web authentication entries exist, and users of other authentication types fail authentication or fail to get authorized when a large number of users exist.
- Condition: This symptom might occur if the following operations are performed when Web authentication is disabled:
  a. Configure the web-auth free-ip command.
  b. Reboot the device.

201710310028

- Symptom: In an IRF fabric, the RRPP convergence time is 6 to 10 seconds after a master/subordinate switchover is performed upon a master reboot.
- Condition: This symptom occurs if two RRPP domains are configured on the IRF fabric.

201710270144

- Symptom: The device fails to automatically execute the **save force** command.
- Condition: This symptom might occur if the **save force** command is added to the autocfg configuration file.

201704280459

- Symptom: CVE-2017-6458
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201704280459

- Symptom: CVE-2016-9042
- Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

201704270120

- Symptom: CVE-2014-9297

- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.

201704270120

- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201705040699

- Symptom: The MAC learning priority settings do not take effect. An interface with low MAC address learning priority can learn the MAC addresses that have been learned by an interface with high MAC address learning priority.
- Condition: This symptom might occur if the source MAC addresses of Layer 2 packets received on the low-priority interface are the same with the high-priority interface.

201707140396

- Symptom: An authenticated user fails MAC authentication when the user attempts to come online again after the switch reboots.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable port security and set the port security mode of a port to macAddressWithRadius, macAddressOrUserLoginSecure, macAddressElseUserLoginSecure, macAddressOrUserLoginSecureExt, or macAddressElseUserLoginSecureExt.
  b. A user passes MAC authentication on the port.
  c. Save the running configuration to a configuration file, set the configuration file as the next startup configuration file, and delete the .mdb configuration file.
  d. Reboot the switch.

201705120786

- Symptom: When an interface is configured with broadcast, multicast, and unknown unicast storm suppression, the storm suppression thresholds cannot be modified in a specific sequence.
- Condition: This symptom might occur if the following operations are performed:
  a. Enable broadcast, multicast, and unknown unicast storm suppression on an interface and set the storm suppression thresholds in percentage to 0 for the three traffic types.
  b. Change the storm suppression threshold unit for a traffic type from percentage to pps.
  c. Disable unknown unicast storm suppression.

201707260794

- Symptom: Traffic forwarding fails because some L3 entries having parity errors cannot berecovered.
- Condition: This symptom might occur if some L3 entries have parity errors.

201708310228

- Symptom: Packet filtering does not work after the switch is rebooted.
- Condition: This symptom might occur if the switch is rebooted after packet filtering is configured.

201710200579

- Symptom: After a Layer 2 extended-link aggregation group is deleted, only one of its former member ports can forward broadcast traffic.
- Condition: This symptom might occur if a Layer 2 extended-link aggregation group is deleted.

201709220068

- Symptom: On an IRF fabric, the view of some interfaces might be unavailable after an IRF master/subordinate switchover.
- Condition: This symptom might occur if an IRF master/subordinate switchover occurs when a new member joins the IRF fabric.

201709040292

- Symptom: With the HWTACACS accounting server being blocked, the switch responds slowly to commands input by a Telnet user.
- Condition: This symptom might occur if HWTACACS authentication is enabled for login.

201710270540

- Symptom: Certain QoS policies cannot be applied.
- Condition: This symptom might occur if one of the following operations are performed.
  - Apply a QoS policy that matches the outer VLAN IDs or inner VLAN IDs to the inbound direction of an interface for outer VLAN ID remarking.
  - Apply a QoS policy that matches the inner VLAN IDs to the inbound direction of an interface for inner VLAN ID remarking.
  - Apply a QoS policy that matches the outer VLAN IDs to the outbound direction of an interface for inner VLAN ID remarking.

201710200099

- Symptom: sFlow cannot collect outgoing traffic statistics on an interface.
- Condition: This symptom might occur if sFlow is configured on an interface.

201709250190

- Symptom: In a Layer 2 extended-link aggregation group, broadcast traffic received by a member port is forwarded out of the other member ports.
- Condition: This symptom might occur if a member port of a Layer 2 extended-link aggregation group receives broadcast traffic.

201709010571

- Symptom: LLDP is enabled globally and on an interface. The LLDPDUs sent by the interface show that autonegotiation is supported and enabled, but the PMD parameter Auto-negotiated Advertised Capability field is all zeros.
- Condition: This symptom might occur if LLDP is enabled globally and on an interface.

Resolved problems in R1309

201704280459

- Symptom: CVE-2017-6458
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

201704280459

- Symptom: CVE-2016-9042
- Condition: NTP is prone to a denial-of-service vulnerability. An attacker can exploit this issue to cause a denial-of-service condition, denying service to legitimate users.

201704270120

- Symptom: CVE-2014-9297

- Condition: An attacker can exploit this issue. When an NTP client decrypted a secret received from an NTP server.

201704270120

- Symptom: CVE-2015-9298
- Condition: An attacker could bypass source IP restrictions and send malicious control and configuration packets.

201707260794

- Symptom: Forwarding errors or traffic interruptions might occur on the switch.
- Condition: This symptom occurs with a low probability if the switch runs for a long time.

201707200766

- Symptom: During automatic ADCampus deployment, the switch does not replace the configuration on a downlink interface with the trunk port configuration when an AP accesses the switch through the downlink interface.
- Condition: This symptom might occur if the switch acts as an access node on the ADCampus network.

201707170566

- Symptom: The value of the **MaxPower** field is incorrect in the output from the **display poe device** command.
- Condition: This symptom might occur if the switch is enabled with PoE.

201707170562

- Symptom: In an IRF fabric, IRF physical interfaces keep receiving packets with a CRC error.
- Condition: This symptom might occur if fixed 40-GE ports on the switch panel are used as the IRF physical interfaces.

201707150289

- Symptom: When uRPF is globally enabled, the switch does not forward packets of which the source IP addresses match the destination addresses of non-direct routing entries.
- Condition: This symptom might occur if the switch is globally enabled with uRPF.

201703090716

- Symptom: The DHCP snooping trusted port configuration does not take effect on an aggregate interface on a multi-chassis IRF fabric.
- Condition: This symptom might occur if the following operations are performed on the IRF fabric:
  a. Configure an aggregate interface as a DHCP snooping trusted port.
  b. Initiate an IRF master/subordinate switchover. Or, save the running configuration and reboot the IRF fabric.

Resolved problems in R1308

None

Resolved problems in R1121P03

201610140261

- Symptom: CVE-2016-6304

- Condition: OpenSSL is prone to denial-of-service vulnerability. An attacker may exploit this issue to cause a denial-of-service condition.

201610140261

- Symptom: CVE-2016-6306
- Condition: OpenSSL is prone to a local denial-of-service vulnerability. A local attacker can exploit this issue to cause a denial-of-service condition.

Resolved problems in R1121P02

201610260405

- Symptom: A user fails to log in to the switch in SSH or Telnet method.
- Condition: This symptom occurs if the following conditions exist:
  - The switch is configured with the tcp syn-cookie enable command.
  - The SSH/Telnet client is not directly connected to the switch.
  - A user remotely logs in to the switch by using the IPv6 address of the switch in SSH or Telnet method.

201607180428

- Symptom: IS-IS neighbor relationship can be established between a switch and a Cisco NX9000 device. However, the switch cannot get routing information.
- Condition: This symptom occurs if the following conditions exist:
  - The switch and the Cisco NX9000 device are connected by using IS-IS.
  - The length of the MT IS TLV in protocol packets sent by the Cisco NX9000 device is 2 bytes. The switch considers the LSPs as invalid and drops them.

201603280338

- Symptom: The switch and the firewall module installed in the switch might fail to ping each other.
- Condition: This symptom occurs if the firewall module LSPM6FWD is repeatedly rebooted.

201607080484

- Symptom: The enhanced CDP feature deletes unauthenticated voice users.
- Condition: This symptom occurs if the MAC authentication delay feature is enabled.

201606210088

- Symptom: A voice VLAN user cannot join the critical voice VLAN.
- Condition: This symptom occurs if the switch receives CDP packets from some IP phones.

201611210490

- Symptom: An interface on an LSWM2SP2PM interface card cannot come up.
- Condition: This symptom occurs if the following conditions exist:
  - The switch has an LSWM2SP2PM interface card installed.
  - MACsec is configured on an interface of the interface card.
  - The switch is rebooted.

201610240043

- Symptom: The configuration fails to be saved.

- Condition: This symptom occurs if the **storm-constrain** command configuration flag bit in the memory is modified.

201610150088

- Symptom: A user cannot access the network after passing MAC authentication.
- Condition: This symptom occurs if the following operations are performed:
  a. Enable MAC authentication for access users.
  b. Enable MAC move.
  c. Configure an IRF fabric and then forward traffic on only one IRF member device.

201610100067

- Symptom: A TFTP operation failure log is displayed even if the TFTP operation succeeds.
- Condition: This symptom occurs if a TFTP operation is performed.

201610310115

- Symptom: The speed of a 1000-Mbps port is negotiated as 100 Mbps when it is connected to a 1000-Mbps NIC.
- Condition: This symptom occurs if a 1000-Mbps copper port is connected to a 1000-Mbps NIC of a server.

Resolved problems in R1121P01

201607280524

- Symptom: CVE-2016-2177
- Condition: Fixed vulnerability in s3_srvr.c, ssl_sess.c, and t1_lib.c functions in OpenSSL through 1.0.2h that allows remote attackers to cause a denial of service (integer overflow and application crash), or possibly have an unspecified other impact by leveraging unexpected malloc behavior.

201608290241

- Symptom: CVE-2009-3238
- Condition: The get_random_int function in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms.

201609060439

- Symptom: BFD MAD is in faulty state on an IRF fabric when certain conditions exist.
- Condition: This symptom might occur if BFD MAD is configured on an IRF fabric and its peer, and the IRF fabric can receive BFD packets from the peer.

201609230495

- Symptom: After frequent Telnet or SSH logins and logouts, the following symptoms might occur when the patch for the comsh process is installed:
  - In standalone mode, patch installation takes a long period of time.
  - In IRF mode, if the patch is first installed on the master, patch installation takes a long period of time; if the patch is first installed on subordinates, patch installation fails on the master.
- Condition: This symptom might occur if frequent Telnet or SSH logins and logouts are performed.

201608110180

- Symptom: On an IRF fabric, when the memory usage of the master exceeds the upper limit, BGP NSR might have unrecoverable errors.
- Condition: This symptom might occur if BGP is configured on an IRF fabric, and the memory usage of the master exceeds the upper limit.

201606270545

- Symptom: When multiple MD5 authentication modes are configured for an OSPF area, the switch has PW errors and fails to establish neighbor relationships after a reboot.
- Condition: This symptom might occur if multiple MD5 authentication modes are configured for an OSPF area.

201607180448

- Symptom: When a traceroute operation is performed on a remote device, and the switch is on the path to the destination, the remote device cannot detect the switch, and the switch displays the "ICMP Discard: ICMP reached rate limit." message.
- Condition: This symptom might occur if a traceroute operation is performed on a remote device, and the switch is on the path to the destination.

201610130001

- Symptom: In the help information of the **mtu** command, the MTU value range is incorrect.
- Condition: This symptom might occur if the help information is displayed for the **mtu** command.

201609210504

- Symptom: In the help information of the **jumboframe enable** command, the maximum frame length is not 12000.
- Condition: This symptom might occur if the help information is displayed for the **jumboframe enable** command.

201607220132

- Symptom: After the switch is powered off and rebooted, information is modified for some transceiver modules that are not write-protected, and the transceiver modules become unavailable because of damage.
- Condition: This symptom might occur if the switch is powered off and rebooted.

201606270084

- Symptom: The switch does not process EAPOL v3 packets of 802.1X authentication and displays the "Invalid protocol version ID" message.
- Condition: This symptom might occur if the switch receives EAPOL v3 packets of 802.1X authentication.

201609280505

- Symptom: The settings of a RADIUS scheme are saved twice on an IRF fabric. After a master/subordinate switchover, the RADIUS scheme settings are lost.
- Condition: This symptom might occur if the settings of a RADIUS scheme are saved twice on an IRF fabric, and a master/subordinate switchover occurs.

201608110180

- Symptom: The status of BGP NSR is not correct and cannot recover.
- Condition: This symptom occurs if BGP NSR is configured for an IRF fabric and the memory threshold is reached.

201607180405

- Symptom: The CLI hangs.
- Condition: This symptom occurs if the following conditions exists:
  - CDP compatibility for LLDP is enabled on the device.
  - A port is configured to be shut down upon receiving an illegal frame.
  - The port is connected to a Cisco telephone, and the telephone fails authentication.

201609010307

- Symptom: No authentication page is pushed when a user performs portal authentication.
- Condition: This symptom occurs if the following conditions exist:
  - Portal authentication is configured on the device.
  - The user tries to access the external network through a Web browser on the PC connected to the device.

201609030158

- Symptom: The device does not receive any OpenFlow entries from the OpenFlow controller.
- Condition: This symptom occurs if the OpenFlow controller is an open-source SDN controller.

201607270178

- Symptom: 802.1X or MAC authentication users on an IRF fabric cannot come online.
- Condition: This symptom occurs if the following conditions exist:
  - The maximum number of 802.1X or MAC authentication users on the IRF fabric is reached.
  - The users that pass 802.1X or MAC authentication but do not obtain authorized rights go offline, because an IRF master/subordinate switchover occurs or interfaces go down.

201609130493

- Symptom: An error message does not end with a new line character.
- Condition: This symptom occurs when you associate an interface that does not support VPN with a VPN instance.

Resolved problems in R1121

201605040255

- Symptom: CVE-2015-8138
- Condition: Fixed vulnerability in ntpd which attackers may be able to disable time synchronization by sending a crafted NTP packet to the NTP client.

201605040255

- Symptom: CVE-2015-7979
- Condition: Fixed vulnerability in ntpd allows attackers to send special crafted broadcast packets to broadcast clients, which may cause the affected NTP clients to become out of sync over a longer period of time.

201605040255

- Symptom: CVE-2015-7974
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201605040255

- Symptom: CVE-2015-7973
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201607280521

- Symptom: CVE-2012-0036
- Condition: Fixed vulnerability in curl and libcurl 7.2x before 7.24.0 that allows remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection attack on the (1) IMAP, (2) POP3, or (3) SMTP protocol.

201606280241

- Symptom: CVE-2016-4953
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending a spoofed packet with incorrect authentication data at a certain time.

201606280241

- Symptom: CVE-2016-4954
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.

201606280241

- Symptom: CVE-2016-4956
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service via a spoofed broadcast packet.

01608260185

- Symptom: The new master device in an IRF fabric hangs after a master/subordinate switchover.
- Condition: This symptom occurs if the following tasks are performed:
  a. Reboot the master device in the IRF fabric. A master/subordinate switchover occurs.
  b. Wait for IRF physical interfaces on the previous master device to come up.
  c. Walk MIB node hh3cStackPortStatus.

201609070244

- Symptom: PD detection and classification on a port are affected after PoE performs power negotiation on the port.
- Condition: None.

201606270528

- Symptom: The device might reboot unexpectedly.
- Condition: This symptom occurs if a user with an ultra-long username Telnets to the device.

201606270484

- Symptom: The description configuration for an interface fails, but no error message is displayed.
- Condition: This symptom occurs if the description contains Chinese characters.

201606070262

- Symptom: The device configured with OpenFlow inband management VLANs cannot establish OSPF or OSPFv3 neighbor relationships with other devices.
- Condition: This symptom occurs if the device is configured with OpenFlow inband management VLANs.

201608170255

- Symptom: Packet statistics for a management Ethernet interface are incorrect.
- Condition: This symptom occurs if the statistics are obtained through MIB.

201607190428

- Symptom: The speed autonegotiation configuration is lost.
- Condition: This symptom occurs if the .mdb next-startup configuration file is deleted and the device starts up with a .cfg next-startup configuration file.

201607110099

- Symptom: Maximum PI power negotiation fails on an interface configured with PoE.
- Condition: This symptom occurs if the maximum PI power is automatically deployed on the interface and the device is rebooted after the configuration is saved.

201607040331

- Symptom: A user that fails MAC authentication cannot be assigned to the MAC authentication critical VLAN on the access port of the user.
- Condition: This symptom occurs if the following conditions exists:
  - The user fails MAC authentication and is assigned to the MAC authentication guest VLAN on the port.
  - The authentication server becomes unreachable.
  - Users are removed from the MAC authentication guest VLAN on the port by using the reset mac-authentication guest-vlan command.

Resolved problems in R1120P10

201606150036

- Symptom: After the switch is powered off and then rebooted, some transceiver modules without write protection are damaged.
- Condition: This symptom might occur if the switch is powered off and then rebooted.

201605120341

- Symptom: Traffic forwarding fails because some L3 entries having parity errors cannot be recovered.
- Condition: This symptom might occur if some L3 entries have parity errors.

201604180493

- Symptom: ACLs that use a rule containing the **established** parameter do not take effect when they are used with 802.1X authentication or MAC authentication.
- Condition: This symptom might occur if 802.1X authentication or MAC authentication is enabled.

201604120327

- Symptom: The switch does not generate the MAC_TABLE_FULL_PORT log message when the MAC learning limit is reached on an interface enabled with voice VLAN.

- Condition: This symptom might occur if the **mac-address max-mac-count** command is configured on an interface enabled with voice VLAN.

201606210245

- Symptom: In the output from the **display ip routing-table** command, OSPF internal routes and external routes are not differentiated.
- Condition: This symptom might occur if the **display ip routing-table** command is executed.

201606060110

- Symptom: A ping operation through a management Ethernet interface fails when ICMP echo requests are longer than 1472 bytes.
- Condition: This symptom might occur if a ping operation is performed through a management Ethernet interface and ICMP echo requests are longer than 1472 bytes.

201604180513

- Symptom: When inactivity aging of port security is enabled on an interface, a sticky MAC address ages out before the secure MAC aging timer expires.
- Condition: This symptom might occur if the following conditions exist on an interface:
  - Port security and inactivity aging are enabled.
  - The port-security timer autolearn aging command is used to set the secure MAC aging timer.

201603190339

- Symptom: When RADIUS server load sharing is enabled, multiple RADIUS packets for one 802.1X EAP authentication process are sent to different RADIUS servers.
- Condition: This symptom might occur if RADIUS server load sharing is enabled.

201604180531

- Symptom: A PC cannot join the 802.1X guest VLAN.
- Condition: This symptom occurs if the following conditions exist:
  - Both 802.1X authentication and MAC authentication are enabled on the device.
  - The device connects to multiple PCs through a hub.
  - The PC fails MAC authentication.

201607020041

- Symptom: The entPhysicalModelName node displays the information for the subslot instead of the information for CPU 0 in slot 1 during a MIB walk.
- Condition: This symptom occurs if a MIB walk is performed on the entPhysicalModelName node.

201606230218

- Symptom: Dynamically learned secure MAC addresses of a port cannot be deleted after the port goes down.
- Condition: This symptom occurs if the port is enabled with the dynamic secure MAC feature.

201606220123

- Symptom: A user that fails 802.1X authentication for the first time fails subsequent 802.1X authentication.
- Condition: This symptom occurs if the user comes online after passing MAC authentication and then performs 802.1X authentication.

201604260373

- Symptom: The actual period of traffic interruption is three seconds rather than six seconds after a port is disconnected and then reconnected.
- Condition: This symptom occurs if the LACP short timeout interval is set for the port.

201605090524

- Symptom: CVE-2015-7979
- Condition: Fixed vulnerability in ntpd allows attackers to send special crafted broadcast packets to broadcast clients, which may cause the affected NTP clients to become out of sync over a longer period of time.

201605090524

- Symptom: CVE-2015-7974
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201605090524

- Symptom: CVE-2015-7973
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201606070567

- Symptom: CVE-2016-2105
- Condition: Fixed vulnerability in “EVP Encode” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

201606070567

- Symptom: CVE-2016-2106
- Condition: Fixed vulnerability in “EVP Encrypt” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

201606070567

- Symptom: CVE-2016-2107
- Condition: Fixed vulnerability in OpenSSL before 1.0.1t and 1.02h allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.

201606070567

- Symptom: CVE-2016-2108
- Condition: Fixed vulnerability in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption).

201606070567

- Symptom: CVE-2016-2109
- Condition: Fixed vulnerability in “asn” before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.

201606070567

- Symptom: CVE-2016-2176

- Condition: Fixed vulnerability in “X509” in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from memory or cause a denial of service

201605170546

- Symptom: CVE-2016-1547
- Condition: Fixed vulnerability where an off-path attacker can deny service to ntpd clients by demobilizing preemptable associations using spoofed crypto-NAK packets.

201605170546

- Symptom: CVE-2016-1548
- Condition: Fixed vulnerability where an attacker can change the time of an ntpd client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode.

201605170546

- Symptom: CVE-2016-1550
- Condition: Fixed vulnerability in ntpd function allow an attacker to conduct a timing attack to compute the value of the valid authentication digest causing forged packets to be accepted by ntpd.

201605170546

- Symptom: CVE-2016-1551
- Condition: Fixed vulnerability in ntpd allows unauthenticated network attackers to spoof refclock packets to ntpd processes on systems that do not implement bogon filtering.

201605170546

- Symptom: CVE-2016-2519
- Condition: Fixed vulnerability in ntpd will abort if an attempt is made to read an oversized value.

201605170546

- Symptom: CVE-2015-7704
- Condition: Fixed vulnerability in ntpd that a remote attacker could use, to send a packet to an ntpd client that would increase the client's polling interval value, and effectively disable synchronization with the server.

Resolved problems in R1120P07

201601140410

- Symptom: When TCP port X is enabled, TCP port X + 2048*N is also enabled (N is an arbitrary integer).
- Condition: This symptom occurs if TCP port X is enabled, for example, TCP port 23 is enabled by using the **telnet server enable** command.

201602150295

- Symptom: After the switch is rebooted, the configuration for queue **a** in a custom queue scheduling profile is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Use the qos qmprofile command to create a custom queue scheduling profile.
  b. Configure queue a to use SP queuing.
  c. Modify the queuing configuration to WRR or WFQ for queue a.

d. Save the configuration and reboot the switch.

201603190098

- Symptom: If you assign a Layer 2 Ethernet interface to Layer 2 aggregation group 2 after assigning it to Layer 2 aggregation group 1, the configuration fails, and all link aggregation group configuration on the interface is deleted.
- Condition: This symptom occurs if the following operations are performed:
  a. Assign a Layer 2 Ethernet interface to Layer 2 aggregation group 1.
  b. Assign the interface to Layer 2 aggregation group 2.

201603110390

- Symptom: The message "The operation completed unsuccessfully." appears when the **undo port auto-power-down** command is executed on an interface.
- Condition: This symptom occurs if the **undo port auto-power-down** command is executed on an interface.

201603160134

- Symptom: A DHCP client cannot obtain an IP address.
- Condition: This symptom occurs if the following conditions exist:
  - DHCP snooping is enabled on a switch.
  - DHCP request messages are forwarded across VLANs on the DHCP snooping-enabled switch.

201603180570

- Symptom: After a PC joins the critical VLAN, the PC is reauthenticated about every 20 seconds.
- Condition: This symptom occurs if the 802.1X server is unreachable when the PC performs 802.1X authentication.

201604210202

- Symptom: A PC is logged out immediately after the PC successfully comes online through 802.1X authentication.
- Condition: This symptom occurs if the following conditions exist:
  - An IP phone comes online through MAC authentication.
  - The PC is connected to the switch through the IP phone.
  - The PC performs 802.1X authentication, and no authorization VLAN is assigned to the PC.

201604180493

- Symptom: When an ACL of the established type is issued, the system prompts that the ACL is not supported.
- Condition: This symptom occurs if 802.1X or MAC authentication is enabled and the switch issues an ACL of the established type.

201603190309

- Symptom: The **dot1x re-authenticate server-unreachable keep-online** command configuration does not take effect. When the server is unreachable, the user is reauthenticated and then logged out.
- Condition: This symptom occurs if the **dot1x re-authenticate server-unreachable keep-online** command is configured and the session timeout timer is triggered after the user comes online.

201603180515

- Symptom: CVE-2016-0701

- Condition: Fixed vulnerability in the DH_check_pub_key function which makes it easier for remote attackers to discover a private DH (Diffie-Hellman) exponent by making multiple handshakes with a peer that chose an inappropriate number. This issue affects OpenSSL version 1.0.2. and addressed in 1.0.2f. OpenSSL 1.0.1 is not affected by this CVE.

201603180515

- Symptom: CVE-2015-3197
- Condition: Fixed vulnerability when using SSLv2 which can be exploited in a man-in-the-middle attack, if device has disabled ciphers.

201603230415

- Symptom: CVE-2016-0705
- Condition: Fixed vulnerability when OpenSSL parses malformed DSA private keys and could lead to a DoS attack or memory corruption for applications that receive DSA private keys from untrusted sources.

201603230415

- Symptom: CVE-2016-0798
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt.

201603230415

- Symptom: CVE-2016-0797
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference).

201603230415

- Symptom: CVE-2016-0799
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service which could lead to memory allocation failure or memory leaks.

201603230415

- Symptom: CVE-2016-0702
- Condition: Fixed vulnerability in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g which makes it easier for local users to discover RSA keys leveraging cache-bank conflicts, aka a "CacheBleed" attack.

201604110488

- Symptom: CVE-2016-2842
- Condition: Fixed vulnerability in the doapr_outch function in crypto/bio/b_print.c, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string.

201604060219

- Symptom: When DHCP server and DHCP snooping settings are configured on the switch, DHCP clients can obtain IP addresses, but the switch cannot generate DHCP snooping entries.
- Condition: This symptom might occur if DHCP server and DHCP snooping settings are configured on the switch.

201603090119

- Symptom: An ACL rule takes effect 25 seconds later than the start time of the time range specified for the rule.
- Condition: None.

201512110325

- Symptom: The listening TCP port configuration on a local portal Web server changes to the default setting after the local portal Web server view is re-entered.
- Condition: This symptom occurs if the local portal Web server uses HTTPS to exchange authentication information with clients.

201601260436

- Symptom: A dynamic aggregate interface goes down and then comes up after the receiver or transmitter of the transceiver module on one of its member port is removed.
- Condition: This symptom occurs if BFD is configured on the aggregate interface.

201601050377

- Symptom: The **switch-mode** command configuration for ARP tables does not take effect on VLAN interfaces configured as customer-side ports by using the **arp mode uni** command.
- Condition: None.

201603010069

- Symptom: The **Session timeout period** field in the **display mac-authentication connection** command output displays **N/A**.
- Condition: This symptom might occur if the authentication server assigns the Session-Timeout attribute.

201603160269

- Symptom: The switch fails to establish an LDP LSP with the peer device after LDP is disabled and then enabled on the peer port.
- Condition: This symptom occurs if the peer port is configured with a secondary IP address.

Resolved problems in R1120

201512290191

- Symptom: CVE-2015-3194
- Condition: The signature verification routines will crash with a NULL pointer dereference, if presented with an ASN.1 signature using the RSA PSS algorithm and absent mask generation function parameter. This can be used to crash any certificate verification operation and exploited in a DoS attack.

201512290191

- Symptom: CVE-2015-3195
- Condition: When presented with a malformed X509_ATTRIBUTE structure OpenSSL will leak memory. This structure is used by the PKCS#7 and CMS routines so any application which reads PKCS#7 or CMS data from untrusted sources is affected.

201512290191

- Symptom: CVE-2015-3196

- Condition: If PSK identity hints are received by a multi-threaded client then the values are wrongly updated in the parent SSL_CTX structure. This can result in a race condition potentially leading to a double free of the identify hint data.

201512290191

- Symptom: CVE-2015-1794
- Condition: If a client receives a ServerKeyExchange for an anonymous DH ciphersuite with the value of p set to 0 then a seg fault can occur leading to a possible denial of service attack.

201512150528

- Symptom: NTP clock synchronization fails.
- Condition: This symptom occurs if the switch is connected to an NTP-enabled Cisco device.

201603010337

- Symptom: After a static default route is configured, packets destined for invalid class-E IP addresses are forwarded rather than dropped.
- Condition: This symptom occurs if a static default route is configured and the switch receives packets destined for invalid class-E IP addresses.

201602150295

- Symptom: After the switch is rebooted, the configuration for a queue in a user-defined queue scheduling profile is lost.
- Condition: This symptom occurs if the following operations are performed:
  a. Use the qos qmprofile command to create a user-defined queue scheduling profile.
  b. Configure the queuing method as SP for the queue in the queue scheduling profile.
  c. Modify the queuing method to WRR or WFQ for the queue in the queue scheduling profile.
  d. Save the configuration and reboot the switch.

201510300359

- Symptom: When an MAC authentication user is online, an 802.1X user goes offline immediately after the user passes 802.1X authentication and comes online.
- Condition: This symptom occurs if MAC authentication and 802.1X authentication assign the same VLAN to users.

201509220038

- Symptom: User authentication fails.
- Condition: This symptom occurs if the switch uses an ACS 5.6 server to perform AAA authentication.

Resolved problems in R1118P02

201511200517

- Symptom: CVE-2015-7871
- Condition: Cause NTPD to accept time from unauthenticated peers.

201511200517

- Symptom: CVE-2015-7704
- Condition: An NTPD client forged by a DDoS attacker located anywhere on the Internet, which can exploit NTP's to disable NTP at a victim client or it may also trigger a firewall block for packets from the target machine.

201511200517

- Symptom: CVE-2015-7705
- Condition: The DDoS attacker can send a device a high volume of NTPD queries that are spoofed to look like they come from the client. The servers then start rate-limiting the client.

201511200517

- Symptom: CVE-2015-7855
- Condition: NTPD mode 6 or mode 7 packets containing an unusually long data value could possibly use cause NTP to crash, resulting in a denial of service.

201512290083

- Symptom: The **dot1x after-mac-auth max-attempt** command configuration is incorrectly displayed.
- Condition: This symptom might occur if the **dot1x after-mac-auth max-attempt** command is executed.

201512170304

- Symptom: The **boot-loader file** command fails to upgrade the software for all member switches of an IRF fabric at the same time.
- Condition: This symptom might occur if the **boot-loader file** command is used to upgrade the software for all member switches of an IRF fabric at the same time.

201510260061

- Symptom: Users fail 802.1X authentication if the PEAP method is used.
- Condition: This symptom might occur if the PEAP method is used.

Resolved problems in R1118

201511090144

- Symptom: A Cisco IP phone leaves the voice VLAN after LLDP neighbor ages out and the voice VLAN aging timer expires.
- Condition: This symptom occurs if the switch advertises voice VLAN information to the IP phone.

Resolved problems in R1111P01

First release

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 5510 HI Switch Series Installation Guide
- HPE PSR720-56A Power Supply User Guide
- HPE PSR1110-56A Power Supply User Guide
- HPE PSR150-A & PSR150-D Power Supplies User Guide
- HPE LSWM2SP2PM Interface Card (JH157A) User Guide
- HPE LSWM2XGT2PM Interface Card (JH156A) User Guide
- HPE LSWM2QP2P Interface Card (JH155A) User Guide
- HPE 5510 HI Switch Series Configuration Guides-Release 13xx
- HPE 5510 HI Switch Series Command References-Release 13xx

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

Please refer to:

- HPE FlexNetwork 5510 HI Switch Series Installation Guide

Software features

Table 5 Software features of the 5510HI series

Feature	HPE 5510 24G 4SFP+ HI 1-slot Switch JH145A HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch JH147A HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A	HPE 5510 48G 4SFP+ HI 1-slot Switch JH146A HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch JH148A
Full duplex Wire speed L2 switching capacity	288Gbps	336Gbps
Whole system Wire speed L2 switching Packet forwarding rate	214.29Mpps	250Mpps
IRF	• Ring topology • Daisy chain topology • LACP MAD • ARP MAD • ND MAD • BFD MAD	
Link aggregation	• Aggregation of GE ports • Aggregation of 10-GE ports • Aggregation of 40-GE ports • Static link aggregation • Dynamic link aggregation • Inter-device aggregation • A maximum of 128 inter-device aggregation groups • A maximum of 8 ports for each aggregation group	
Flow control	• IEEE 802.3x flow control • Back pressure	
Jumbo Frame	• Supports maximum frame size of 10000	
MAC address table	• 32K MAC addresses • 1K static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a port	

Feature	HPE 5510 24G 4SFP+ HI 1-slot Switch JH145A HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch JH147A HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A	HPE 5510 48G 4SFP+ HI 1-slot Switch JH146A HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch JH148A
VLAN	• Port-based VLANs (4094 VLANs) • QinQ and selective QinQ • Voice VLAN • protocol-vlan • MAC vlan	
VLAN mapping	• One-to-one VLAN mapping • Many-to-one VLAN mapping • Two-to-two VLAN mapping	
ARP	• 16K entries • 2K static entries • Gratuitous ARP • Common proxy ARP and local proxy ARP • ARP source suppression • ARP black hole • ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings) • Multiport ARP	
ND	• 8K entries • 2K static entries • ND Snooping	
VLAN virtual interface	1K	
DHCP	• DHCP client • DHCP snooping • DHCP relay agent • DHCP server • DHCP Option82 • DHCPv6 server • DHCPv6 relay agent • DHCPv6 snooping	
UDP helper	• UDP helper	
DNS	• Static DNS • Dynamic DNS • IPv4 and IPv6 DNS	
unicast route	• IPv4/IPv6 static routes • RIP/RIPng • OSPF/OSPFv3 • BGP/BGP4+ • ISIS/ISISv6 • Routing policies • Policy-based routing	
BFD	• Static route • MAD	

Feature	HPE 5510 24G 4SFP+ HI 1-slot Switch JH145A HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch JH147A HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A	HPE 5510 48G 4SFP+ HI 1-slot Switch JH146A HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch JH148A
Multicast	• IGMP snooping • MLD snooping • IPv4 and IPv6 multicast VLAN • PIM SM • PIM DM • MSDP • IPv4 and IPv6 PIM snooping	
Broadcast/multicast /unicast storm control	• Storm control based on port rate percentage • PPS-based storm control • Bps-based storm control	
MSTP	• STP/RSTP/MSTP protocol • STP Root Guard • BPDU Guard	
SmartLink	• 32	
QoS/ACL	• Remarking of 802.1p and DSCP priorities • Packet filtering at L2 (Layer 2) through L4 (Layer 4) • Eight output queues for each port • SP/WRR/SP+WRR/WDRR/WFQ queue scheduling algorithms • Port-based rate limiting • Flow-based redirection • Time range	
Mirroring	• Stream mirroring • Port mirroring • Multiple mirror observing port • Port remote mirroring (RSPAN)	
Security	• Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • 802.1X • Port security • MAC-address-based authentication • IP Source Guard • HTTPS • PKI • EAD	
802.1X	• Up to 2,048 users • Port-based and MAC address-based authentication • Guest VLAN • Trunk port authentication • Dynamic 802.1X-based QoS/ACL/VLAN assignment	

Feature	HPE 5510 24G 4SFP+ HI 1-slot Switch JH145A HPE 5510 24G PoE+ 4SFP+ HI 1-slot Switch JH147A HPE 5510 24G SFP 4SFP+ HI 1-slot Switch JH149A	HPE 5510 48G 4SFP+ HI 1-slot Switch JH146A HPE 5510 48G PoE+ 4SFP+ HI 1-slot Switch JH148A
Open Flow	• 16 Instance • MAC-IP	
Loading and upgrading	• Loading and upgrading through XModem protocol • Loading and upgrading through FTP • Loading and upgrading through the trivial file transfer protocol (TFTP)	
Management	• Configuration at the command line interface • Remote configuration through Telnet • Configuration through Console port • Simple network management protocol (SNMP) • IMC NMS • System log • Hierarchical alarms • NTP • Power supply alarm function • Fan and temperature alarms	
Maintenance	• Debugging information output • Ping and Tracert • NQA • Track • Remote maintenance through Telnet • 802.1ag • 802.3ah • DLDP • Virtual Cable Test	

Appendix B Upgrading software

This chapter describes types of software used on the switch and how to upgrade software while the switch is operating normally or when the switch cannot correctly start up.

System software file types

Software required for starting up the switch includes:

- **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 software and the startup configuration file or manage files when the switch cannot correctly start up.
- **Software images**—Includes boot images and system images.
  - Boot image—A .bin file that contains the 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 modules required for device operation and some basic features, including device management, interface management, configuration management, and routing management.

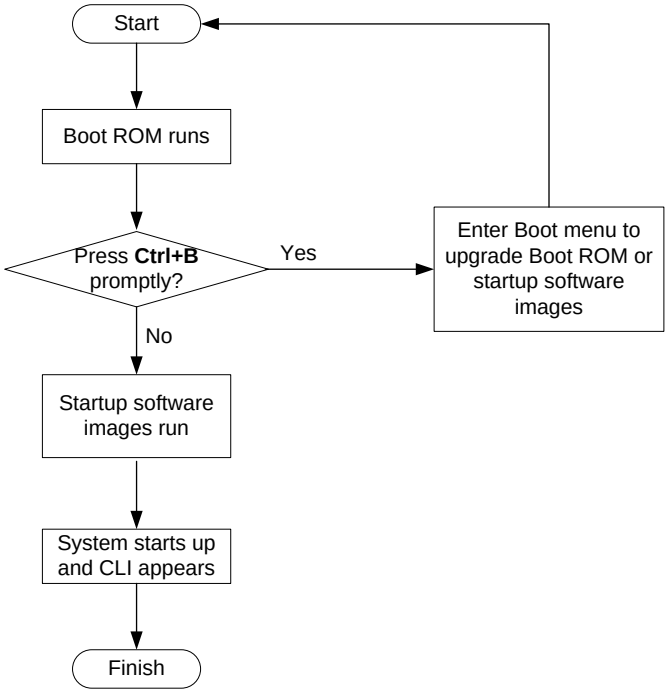
The software images that have been loaded are called “current software images.” The software images specified to load at next startup are called “startup software images.”

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 in the file and sets them as startup software images. Typically, the Boot ROM and software images for this switch series are released in an .ipe file named **main.ipe**.

System startup process

Upon power-on, the Boot ROM image runs to initialize hardware and then the software images run to start up the entire system, as shown in Figure 1.

Figure 1 System startup process



Upgrade methods

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

Upgrading method	Software types	Remarks
Upgrading from the CLI	• Boot ROM image • Software images	• You must reboot the switch to complete the upgrade. • This method can interrupt ongoing network services.
Upgrading from the Boot menu	• Boot ROM image • Software images	Use this method when the switch cannot correctly start up. **△ CAUTION:** Upgrading an IRF fabric from the CLI instead of the Boot menu. The Boot menu method increases the service downtime, because it requires that you upgrade the member switches one by one.

The output in this document is for illustration only and might vary with software releases. This document uses boot.bin and system.bin to represent boot and system image names. The actual software image name format is *chassis-model_Comware-version_image-type_release*, for example, *5510HI-CMW710-BOOT- Rxxxx.bin* and *5510HI-CMW710-SYSTEM-Rxxxx.bin*.

Upgrading from the CLI

This section uses a two-member IRF fabric as an example to describe how to upgrade software from the CLI. If you have more than two subordinate switches, repeat the steps for the subordinate switch to upgrade their software. If you are upgrading a standalone switch, ignore the steps for upgrading the subordinate switch. For more information about setting up and configuring an IRF fabric, see the installation guide and IRF configuration guide for the HPE 5510HI switch series.

Preparing for the upgrade

Before you upgrade software, complete the following tasks:

1. Log in to the IRF fabric through Telnet or the console port. (Details not shown.)
2. Identify the number of IRF members, each member switch's role, and IRF member ID.

```
<Sysname> display irf
MemberID   Role   Priority  CPU-Mac         Description
 *+1       Master 5         0023-8927-afdc  ---
   2       Standby 1        0023-8927-af43  ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-8927-afdb
 Auto upgrade               : no
 Mac persistent             : 6 min
```

```
Domain ID                    : 0
```

3. Verify that each IRF member switch has sufficient storage space for the upgrade images.

IMPORTANT:

Each IRF member switch must have free storage space that is at least two times the size of the upgrade image file.

Identify the free flash space of the master switch.

```
<Sysname> dir
Directory of flash:
     0      -rw-       41424  Aug 23 2013 02:23:44     startup.mdb
     1      -rw-        3792  Aug 23 2013 02:23:44     startup.cfg
     2      -rw-    53555200  Aug 23 2013 09:53:48     system.bin
     3      drw-           -  Aug 23 2013 00:00:07     seclog
     4      drw-           -  Aug 23 2013 00:00:07     diagfile
     5      drw-           -  Aug 23 2013 00:00:07     logfile
     6      -rw-     9959424  Aug 23 2013 09:53:48     boot.bin
     7      -rw-     9012224  Aug 23 2013 09:53:48     backup.bin

524288 KB total (453416 KB free)
```

Identify the free flash space of each subordinate switch, for example, switch 2.

```
<Sysname> dir slot2#flash:/
Directory of slot2#flash:/
     0      -rw-       41424  Jan 01 2011 02:23:44     startup.mdb
     1      -rw-        3792  Jan 01 2011 02:23:44     startup.cfg
     2      -rw-    93871104  Aug 23 2013 16:00:08     system.bin
     3      drw-           -  Jan 01 2011 00:00:07     seclog
     4      drw-           -  Jan 01 2011 00:00:07     diagfile
     5      drw-           -  Jan 02 2011 00:00:07     logfile
     6      -rw-     13611008  Aug 23 2013 15:59:00     boot.bin
     7      -rw-     9012224  Nov 25 2011 09:53:48     backup.bin

524288 KB total (453416 KB free)
```

4. Compare the free flash space of each member switch with the size of the software file to load. If the space is sufficient, start the upgrade process. If not, go to the next step.

5. Delete unused files in the flash memory to free space:

CAUTION:

- To avoid data loss, do not delete the current configuration file. For information about the current configuration file, use the **display startup** command.
- The **delete /unreserved** *file-url* command deletes a file permanently and the action cannot be undone.
- The **delete** *file-url* command moves a file to the recycle bin and the file still occupies storage space. To free the storage space, first execute the **undelete** command to restore the file, and then execute the **delete /unreserved** *file-url* command.

Delete unused files from the flash memory of the master switch.

```
<Sysname> delete /unreserved flash:/backup.bin
The file cannot be restored. Delete flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
```

```
Deleting file flash:/backup.bin...Done.
```

Delete unused files from the flash memory of the subordinate switch.

```
<Sysname> delete /unreserved slot2#flash:/backup.bin
The file cannot be restored. Delete slot2#flash:/backup.bin?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file slot2#flash:/backup.bin...Done.
```

Downloading software images to the master switch

Before you start upgrading software images packages, make sure you have downloaded the upgrading software files to the root directory in flash memory. This section describes downloading an .ipe software file as an example.

The following are ways to download, upload, or copy files to the master switch:

- FTP download from a server
- FTP upload from a client
- TFTP download from a server

Prerequisites

If FTP or TFTP is used, the IRF fabric and the PC working as the FTP/TFTP server or FTP client can reach each other.

Prepare the FTP server or TFTP server program yourself for the PC. The switch series does not come with these software programs.

FTP download from a server

You can use the switch as an FTP client to download files from an FTP server.

To download a file from an FTP server, for example, the server at 10.10.110.1:

1. Run an FTP server program on the server, configure an FTP username and password, specify the working directory and copy the file, for example, **newest.ipe**, to the directory.
2. Execute the **ftp** command in user view on the IRF fabric to access the FTP server.

```
<Sysname> ftp 10.10.110.1
Trying 10.10.110.1...
Press CTRL+C to abort
Connected to 10.10.110.1(10.10.110.1).
220 FTP service ready.
User (10.10.110.1:(none)):username
331 Password required for username.
Password:
230 User logged in.
```

3. Enable the binary transfer mode.

```
ftp> binary
  200 Type set to I.
```

4. Execute the **get** command in FTP client view to download the file from the FTP server.

```
ftp> get newest.ipe
  227 Entering Passive Mode (10,10,110,1,17,97).
  125 BINARY mode data connection already open, transfer starting for /newest.ipe
  226 Transfer complete.
  32133120 bytes received in 35 seconds (896. 0 kbyte/s)
ftp> bye
```

```
221 Server closing.
```

FTP upload from a client

You can use the IRF fabric as an FTP server and upload files from a client to the IRF fabric.

To FTP upload a file from a client:

On the IRF fabric:

1. Enable FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

2. Configure a local FTP user account:

Create the user account.

```
[Sysname] local-user abc
```

Set its password and specify the FTP service.

```
[Sysname-luser-manage-abc] password simple pwd
[Sysname-luser-manage-abc] service-type ftp
```

Assign the **network-admin** user role to the user account for uploading file to the working directory of the server.

```
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
[Sysname-luser-manage-abc] quit
[Sysname] quit
```

On the PC:

3. Log in to the IRF fabric (the FTP server) in FTP mode.

```
c:\> ftp 10.10.110.1
Connected to 10.10.110.1.
220 FTP service ready.
User(10.10.110.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.
```

4. Enable the binary file transfer mode.

```
ftp> binary
200 TYPE is now 8-bit binary.
```

5. Upload the file (for example, **newest.ipe**) to the root directory of the flash memory on the master switch.

```
ftp> put newest.ipe
200 PORT command successful
150 Connecting to port 10002
226 File successfully transferred
ftp: 32133120 bytes sent in 64.58 secs (497.60 Kbytes/sec).
```

TFTP download from a server

To download a file from a TFTP server, for example, the server at 10.10.110.1:

1. Run a TFTP server program on the server, specify the working directory, and copy the file, for example, **newest.ipe**, to the directory.
2. On the IRF fabric, execute the **tftp** command in user view to download the file to the root directory of the flash memory on the master switch.

```
<Sysname> tftp 10.10.110.1 get newest.ipe
Press CTRL+C to abort.
```

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 30.6M    0 30.6M    0     0   143k      0 --:--:--  0:03:38 --:--:--  142k
```

Upgrading the software images

To upgrade the software images:

1. Specify the upgrade image file (**newest.ipe** in this example) used at the next startup for the master switch, and assign the M attribute to the boot and system images in the file.

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
Verifying image file..........Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
Decompressing file boot.bin to flash:/boot.bin...................Done.
Decompressing file system.bin to flash:/system.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. Specify the upgrade image file as the main startup image file for each subordinate switch. This example uses IRF member 2. (The subordinate switches will automatically copy the file to the root directory of their flash memories.)

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
Verifying image file..........Done.
Images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to target slot.
Decompressing file boot.bin to flash:/boot.bin...................Done.
Decompressing file system.bin to flash:/system.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 2.
```

3. Enable the software auto-update function.

```
<Sysname> system-view
[Sysname] irf auto-update enable
[Sysname] quit
```

   This function checks the software versions of member switches for inconsistency with the master switch. If a subordinate switch is using a different software version than the master, the function propagates the current software images of the master to the subordinate as main startup images. The function prevents software version inconsistency from causing the IRF setup failure.

4. Save the current configuration in any view to prevent data loss.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
```

```
Validating file. Please wait.................
Saved the current configuration to mainboard device successfully.
Slot 2:
Save next configuration file successfully.
```

5. Reboot the IRF fabric to complete the upgrade.

```
<Sysname> 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...
```

   The system automatically loads the .bin boot and system images in the .ipe file and sets them as the startup software images.

6. Execute the **display version** command in any view to verify that the current main software images have been updated (details not shown).

NOTE:

The system automatically checks the compatibility of the Boot ROM image and the boot and system images during the reboot. If you are prompted that the Boot ROM image in the upgrade image file is different than the current Boot ROM image, upgrade both the basic and extended sections of the Boot ROM image for compatibility. If you choose to not upgrade the Boot ROM image, the system will ask for an upgrade at the next reboot performed by powering on the switch or rebooting from the CLI (promptly or as scheduled). If you fail to make any choice in the required time, the system upgrades the entire Boot ROM image.

Upgrading from the Boot menu

In this approach, you must access the Boot menu of each member switch to upgrade their software one by one. If you are upgrading software images for an IRF fabric, using the CLI is a better choice.

TIP:

Upgrading through the Ethernet port is faster than through the console port.

Prerequisites

Make sure the prerequisites are met before you start upgrading software from the Boot menu.

Setting up the upgrade environment

1. Use a console cable to connect the console terminal (for example, a PC) to the console port on the switch.
2. Connect the Ethernet port on the switch to the file server.

   NOTE:

   The file server and the configuration terminal can be co-located.

3. Run a terminal emulator program on the console terminal and set the following terminal settings:
   - Bits per second—9,600
   - Data bits—8
   - Parity—None

- Stop bits—1
- Flow control—None
- Emulation—VT100

Preparing for the TFTP or FTP transfer

To use TFTP or FTP:

- Run a TFTP or FTP server program on the file server or the console terminal.
- Copy the upgrade file to the file server.
- Correctly set the working directory on the TFTP or FTP server.
- Make sure the file server and the switch can reach each other.

Verifying that sufficient storage space is available

IMPORTANT:

For the switch to start up correctly, do not delete the main startup software images when you free storage space before upgrading Boot ROM. On the Boot menu, the main startup software images are marked with an asterisk (*).

When you upgrade software, make sure each member switch has sufficient free storage space for the upgrade file, as shown in Table 6.

Table 6 Minimum free storage space requirements

Upgraded images	Minimum free storage space requirements
Comware images	Two times the size of the Comware upgrade package file.
Boot ROM	Same size as the Boot ROM upgrade image file.

If no sufficient space is available, delete unused files as described in "Managing files from the Boot menu."

Scheduling the upgrade time

During the upgrade, the switch cannot provide any services. You must make sure the upgrade has a minimal impact on the network services.

Accessing the Boot menu

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU

********************************************************************************
*                                                                              *
*                 HPE 5510-24G-4SFP+ HI BOOTROM, Version 111                   *
*                                                                              *
********************************************************************************
Copyright (c) 2010-2015 Hewlett-Packard Development Company, L.P.

Creation Date       : Feb  3 2015, 19:43:00
CPU Clock Speed     : 1000MHz
Memory Size         : 2048MB
Flash Size          : 512MB
CPLD Version        : 001
```

```
PCB Version          : Ver.A
Mac Address          : 70f96dfacbda


Press Ctrl+B to access EXTENDED BOOT MENU...0
```

Press one of the shortcut key combinations at prompt.

Table 7 Shortcut keys

Shortcut keys	Prompt message	Function	Remarks
Ctrl+B	Press Ctrl+B to enter Extended Boot menu...	Accesses the extended Boot menu.	Press the keys within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the message appears. You can upgrade and manage system software and Boot ROM from this menu.
Ctrl+D	Press Ctrl+D to access BASIC BOOT MENU	Accesses the basic Boot menu.	Press the keys within 1 seconds after the message appears. You can upgrade Boot ROM or access the extended Boot ROM segment from this menu.

Accessing the basic Boot menu

If the extended Boot ROM segment has corrupted, you can repair or upgrade it from the basic Boot menu.

Press **Ctrl+D** within 1 seconds after the "Press Ctrl+D to access BASIC BOOT MENU" prompt message appears. If you fail to do this within the time limit, the system starts to run the extended Boot ROM segment.

```
********************************************************************************
*                                                                              *
*                          BASIC BOOTROM, Version 111                          *
*                                                                              *
********************************************************************************

   BASIC BOOT MENU

1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
4. Boot extended BootRom
0. Reboot
Ctrl+U: Access BASIC ASSISTANT MENU

Enter your choice(0-4):
```

Table 8 Basic Boot ROM menu options

Option	Task
1. Update full BootRom	Update the entire Boot ROM, including the basic segment and the extended segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
2. Update extended BootRom	Update the extended Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
3. Update basic BootRom	Update the basic Boot ROM segment. To do so, you must use XMODEM and the console port. For more information, see Using XMODEM to upgrade Boot ROM through the console port.
4. Boot extended BootRom	Access the extended Boot ROM segment. For more information, see Accessing the extended Boot menu.
0. Reboot	Reboot the switch.
Ctrl+U: Access BASIC ASSISTANT MENU	Press **Ctrl + U** to access the BASIC ASSISTANT menu (see Table 9).

Table 9 BASIC ASSISTANT menu options

Option	Task
1. RAM Test	Perform a RAM self-test.
0. Return to boot menu	Return to the basic Boot menu.

Accessing the extended Boot menu

Press **Ctrl+B** within 1 second (in fast startup mode) or 5 seconds (in full startup mode) after the "Press Ctrl-B to enter Extended Boot menu..." prompt message appears. If you fail to do this, the system starts decompressing the system software.

Alternatively, you can enter **4** in the basic Boot menu to access the extended Boot menu.

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 10). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE 5510HI Switch Series Configuration Guides*.

```
Password recovery capability is enabled.


   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
```

```
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run

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

Table 10 Extended Boot ROM menu options

Option	Tasks
1. Download image to flash	Download a software image file to the flash.
2. Select image to boot	• Specify the main and backup software image file for the next startup. • Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format file system	Format the current storage medium.
Ctrl+P: Change authentication for console login	Skip the authentication for console login. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
Ctrl+R: Download image to SDRAM and run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT MENU. For options in the menu, see Table 11.

Table 11 EXTENDED ASSISTANT menu options

Option	Task
1. Display Memory	Display data in the memory.

Option	Task
2. Search Memory	Search the memory for a specific data segment.
0. Return to boot menu	Return to the extended Boot ROM menu.

Upgrading Comware images from the Boot menu

You can use the following methods to upgrade Comware images:

- Using TFTP to upgrade software images through the Ethernet port
- Using FTP to upgrade software images through the Ethernet port
- Using XMODEM to upgrade software through the console port

Using TFTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
```

Table 12 TFTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.ipe**).
Server IP Address	IP address of the TFTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

3. Enter all required parameters, and enter **Y** to confirm the settings. The following prompt appears:

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

4. Enter **Y** to start downloading the image file. To return to the Boot menu without downloading the upgrade file, enter **N**.

```
Loading.....................................................................
```

```
.....................................................................
.....................................................................
.....................................................Done!
```

5. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash.....................................................................
.....................................................................
.....................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................Done!
```

NOTE:

- The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images are not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
- If an image with the same attribute as the image you are loading is already in the flash memory, the attribute of the old image changes to none after the new image becomes valid.

6. Enter **0** in the Boot menu to reboot the switch with the new software images.

```
   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run

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

Using FTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **2** to set the FTP parameters.

```
Load File Name      :update.ipe
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
FTP User Name       :switch
FTP User Password   :***
```

Table 13 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.ipe**).
Server IP Address	IP address of the FTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

3. Enter all required parameters, and enter **Y** to confirm the settings. The following prompt appears:

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

4. Enter **Y** to start downloading the image file. To return to the Boot menu without downloading the upgrade file, enter **N**.

```
Loading.....................................................................
.............................................................................
.............................................................................
.....................................................Done!
```

5. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) M
Image file boot.bin is self-decompressing...
Free space: 534980608 bytes
Writing flash...............................................................
```

```
.....................................................................
.....................................................Done!
Image file system.bin is self-decompressing...
Free space: 525981696 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................Done!

   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run

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

NOTE:

- The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images are not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
- If an image with the same attribute as the image you are loading is already in the flash memory, the attribute of the old image changes to none after the new image becomes valid.

6. Enter **0** in the Boot menu to reboot the switch with the new software images.

Using XMODEM to upgrade software through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the Ethernet port. To save time, use the Ethernet port as long as possible.

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **3** to set the XMODEM download baud rate.

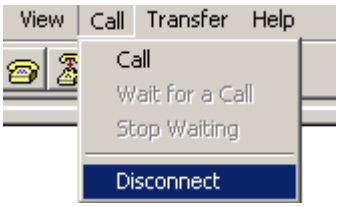
```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu

Enter your choice(0-5):5
```

3. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

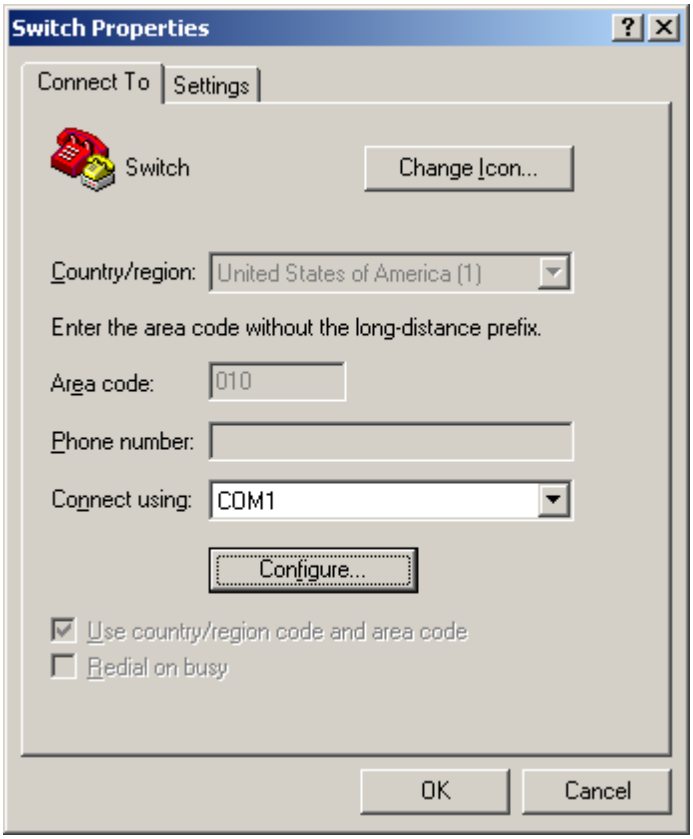
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 2 Disconnecting the terminal from the switch



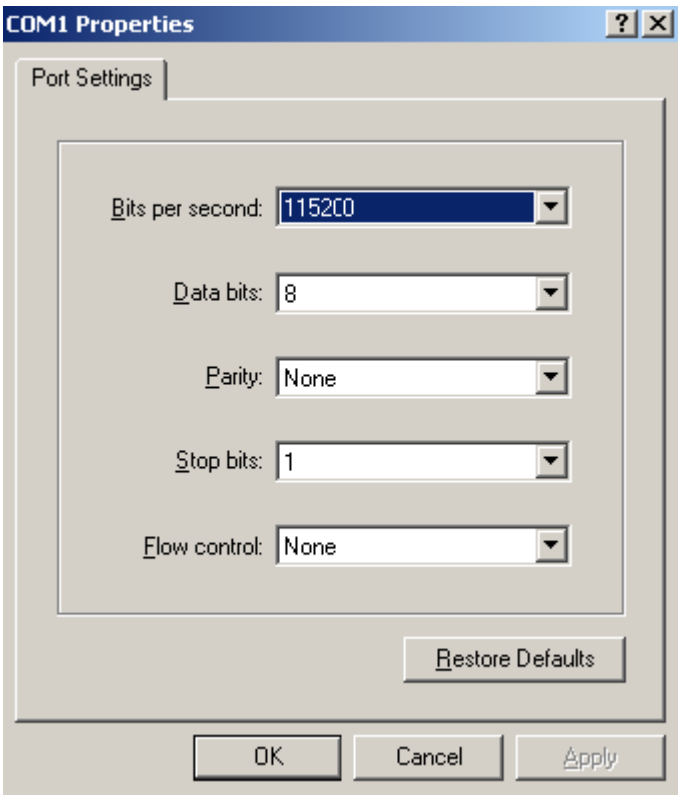
   b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 3 Properties dialog box



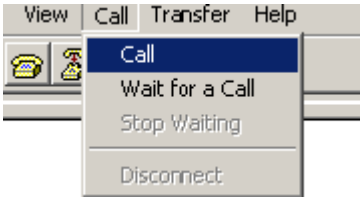
a. Select 115200 from the Bits per second list and click OK.

Figure 4 Modifying the baud rate



a. Select Call > Call to reestablish the connection.

Figure 5 Reestablishing the connection



5. Press **Enter**. The following prompt appears:

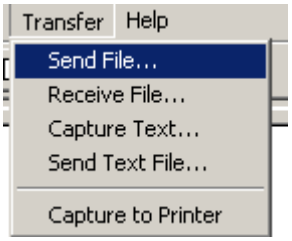
```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

6. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCC
```

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

Figure 6 Transfer menu

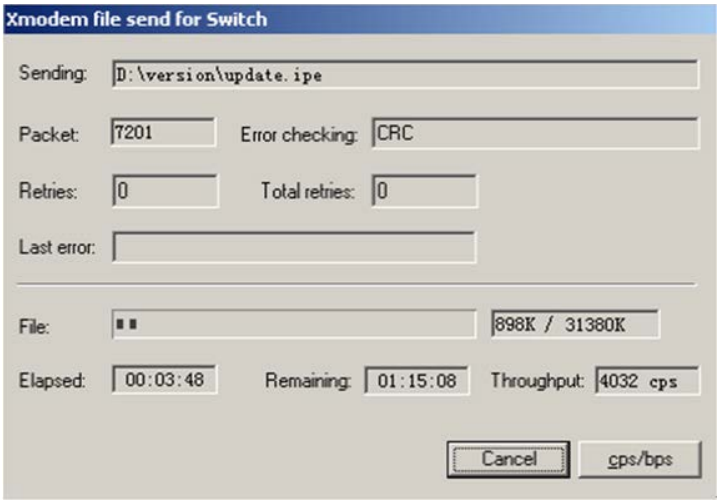


8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 7 File transmission dialog box

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

Figure 8 File transfer progress



10. Enter the **M** (main), **B** (backup), or **N** (none) attribute for the images. In this example, assign the main attribute to the images.

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
```

At the **Load File name** prompt, enter a name for the boot image to be saved to flash memory.

```
Load File name  : default_file boot-update.bin       (At the prompt,
Free space: 470519808 bytes
Writing flash.....................................................................
.............Done!
The system-update.bin image is self-decompressing...
```

At the **Load File name** prompt, enter a name for the system image to be saved to flash memory.

```
Load File name  : default_file system-update.bin
Free space: 461522944 bytes
Writing flash.....................................................................
.............Done!
Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

NOTE:

- The switch always attempts to boot with the main images first. If the attempt fails, for example, because the main images are not available, the switch tries to boot with the backup images. An image with the none attribute is only stored in the flash memory for backup. To use it at reboot, you must change its attribute to main or backup.
- If an image with the same attribute as the image you are loading is already in flash memory, the attribute of the old image changes to none after the new image becomes valid.

11. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps as described in step 5.a. If the baud rate is 9600 bps, skip this step.

NOTE:

The console port rate reverts to 9600 bps at a reboot. If you have changed the baud rate, you must perform this step so you can access the switch through the console port after a reboot.

```
EXTENDED BOOT MENU
```

```
1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run

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

12. Enter **0** in the Boot menu to reboot the system with the new software images.

Upgrading Boot ROM from the Boot menu

You can use the following methods to upgrade the Boot ROM image:

- Using TFTP to upgrade Boot ROM through the Ethernet port
- Using FTP to upgrade Boot ROM through the Ethernet port
- Using XMODEM to upgrade Boot ROM through the console port

Using TFTP to upgrade Boot ROM through the Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **1** to set the TFTP parameters.

```
Load File Name      :update.btm
Server IP Address   :192.168.0.3
Local IP Address    :192.168.0.2
Subnet Mask         :255.255.255.0
Gateway IP Address  :0.0.0.0
```

Table 14 TFTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.btm**).
Server IP Address	IP address of the TFTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

4. Enter all required parameters and press **Enter** to start downloading the file.

```
Loading.............................................Done!
```

5. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom...........Done.
```

6. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

8. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Using FTP to upgrade Boot ROM through the Ethernet port

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu
```

```
Enter your choice(0-3):
```

3. Enter **2** to set the FTP parameters.

```
Load File Name     :update.btm
Server IP Address  :192.168.0.3
Local IP Address   :192.168.0.2
Subnet Mask        :255.255.255.0
Gateway IP Address :0.0.0.0
FTP User Name      :switch
FTP User Password  :123
```

Table 15 FTP parameter description

Item	Description
Load File Name	Name of the file to download (for example, **update.btm**).
Server IP Address	IP address of the FTP server (for example, 192.168.0.3).
Local IP Address	IP address of the switch (for example, 192.168.0.2).
Subnet Mask	Subnet mask of the switch (for example, 255.255.255.0).
Gateway IP Address	IP address of the gateway (in this example, no gateway is required because the server and the switch are on the same subnet).
FTP User Name	Username for accessing the FTP server, which must be the same as configured on the FTP server.
FTP User Password	Password for accessing the FTP server, which must be the same as configured on the FTP server.

NOTE:

- To use the default setting for a field, press **Enter** without entering any value.
- If the switch and the server are on different subnets, you must specify a gateway address for the switch.

4. Enter all required parameters and press **Enter** to start downloading the file.

```
Loading.............................................Done!
```

5. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

6. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

7. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

8. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Using XMODEM to upgrade Boot ROM through the console port

XMODEM download through the console port is slower than TFTP or FTP download through the Ethernet port. To save time, use the Ethernet port as long as possible.

1. Enter **6** in the Boot menu to access the Boot ROM update menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

2. Enter **1** in the Boot ROM update menu to upgrade the full Boot ROM.

   The file transfer protocol submenu appears:

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

3. Enter **3** to set the XMODEM download baud rate.

```
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu

Enter your choice(0-5):5
```

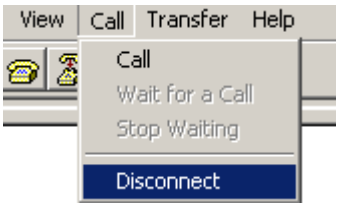
4. Select an appropriate download rate, for example, enter **5** to select 115200 bps.

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

5. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.

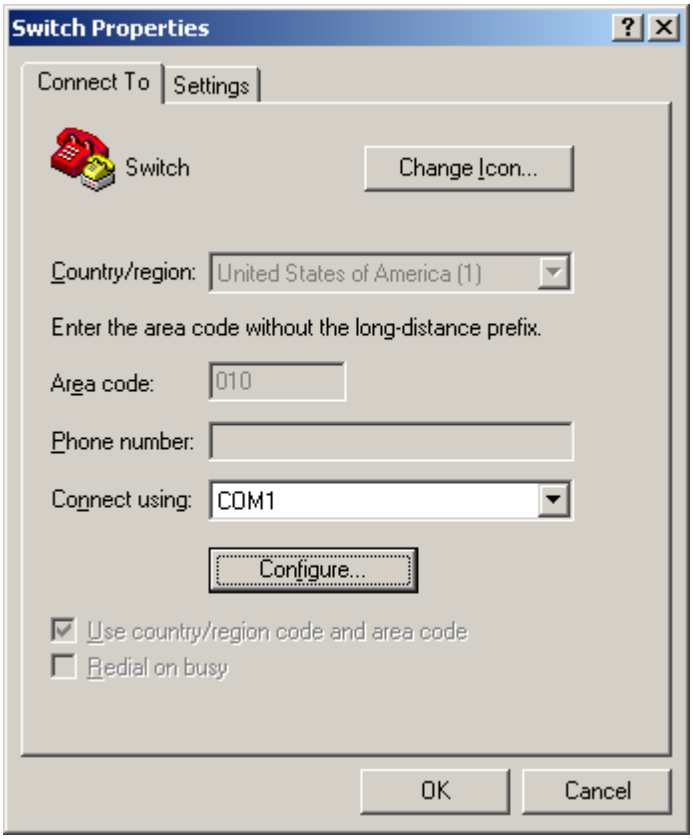
   a. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 9 Disconnecting the terminal from the switch



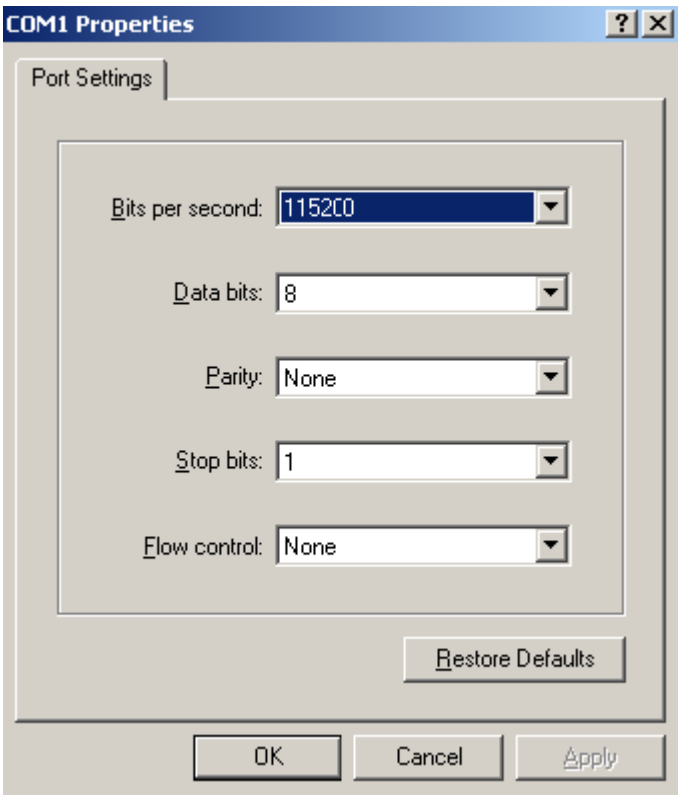
   b. Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 10 Properties dialog box



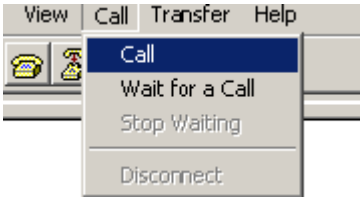
c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 11 Modifying the baud rate



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

Figure 12 Reestablishing the connection

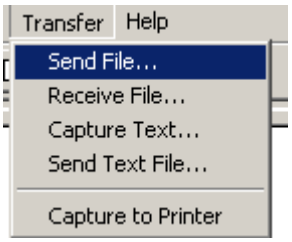


6. Press **Enter** to start downloading the file.

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCC
```

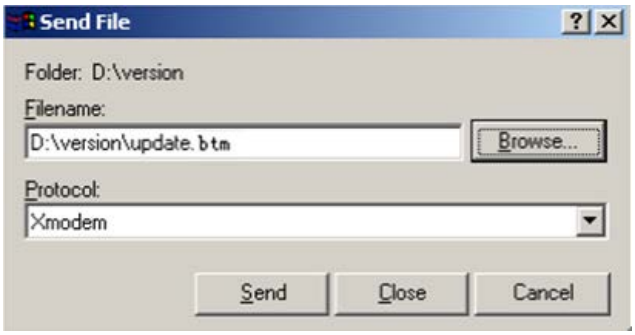
7. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 13 Transfer menu



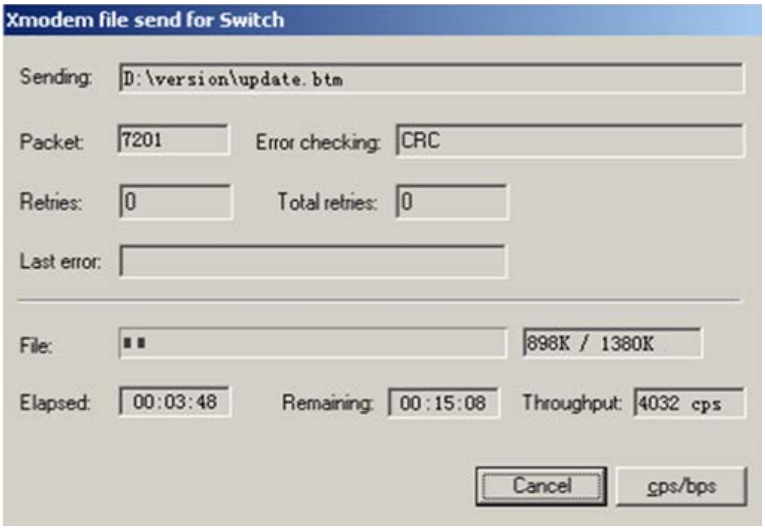
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 14 File transmission dialog box



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

Figure 15 File transfer progress



10. Enter **Y** at the prompt to upgrade the basic Boot ROM section.

```
Loading ...CCCCCCCCCCCCC  ...Done!
Will you Update Basic BootRom? (Y/N):Y
Updating Basic BootRom..........Done.
```

11. Enter **Y** at the prompt to upgrade the extended Boot ROM section.

```
Updating extended BootRom? (Y/N):Y
Updating extended BootRom.........Done.
```

12. If the baud rate of the HyperTerminal is not 9600 bps, restore it to 9600 bps at the prompt, as described in step 4.a. If the baud rate is 9600 bps, skip this step.

```
Please change the terminal's baudrate to 9600 bps, press ENTER when ready.
```

NOTE:

The console port rate reverts to 9600 bps at a reboot. If you have changed the baud rate, you must perform this step so you can access the switch through the console port after a reboot.

13. Press **Enter** to access the Boot ROM update menu.
14. Enter **0** in the Boot ROM update menu to return to the Boot menu.

```
1. Update full BootRom
2. Update extended BootRom
3. Update basic BootRom
0. Return to boot menu

Enter your choice(0-3):
```

15. Enter **0** in the Boot menu to reboot the switch with the new Boot ROM image.

Managing files from the Boot menu

From the Boot menu, you can display files in flash memory to check for obsolete files, incorrect files, or space insufficiency, delete files to release storage space, or change the attributes of software images.

Displaying all files

Enter **3** in the Boot menu to display all files in flash memory and identify the free space size.

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8): 3
```

The following is a sample output:

```
Display all file(s) in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
2(*)           53555200             flash:/system.bin
3(*)           9959424              flash:/boot.bin
4              3678                 flash:/startup.cfg_backup
5              30033                flash:/default.mdb
6              42424                flash:/startup.mdb
7              18                   flash:/.pathfile
8              232311               flash:/logfile/logfile.log
9              5981                 flash:/startup.cfg_back
10(*)          6098                 flash:/startup.cfg
11             20                   flash:/.snmpboots
Free space: 464298848 bytes
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

Deleting files

If storage space is insufficient, delete obsolete files to free up storage space.

To delete files:

1. Enter **4** in the Boot menu:

```
Deleting the file in flash:

File Number    File Size(bytes)     File Name
================================================================================
1              8177                 flash:/testbackup.cfg
```

```
2(*)          53555200            flash:/system.bin
3(*)          9959424             flash:/boot.bin
4             3678                flash:/startup.cfg_backup
5             30033               flash:/default.mdb
6             42424               flash:/startup.mdb
7             18                  flash:/.pathfile
8             232311              flash:/logfile/logfile.log
9             5981                flash:/startup.cfg_back
10(*)         6098                flash:/startup.cfg
11            20                  flash:/.snmpboots
Free space: 464298848 bytes
The current image is boot.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
```

2. Enter the number of the file to delete. For example, enter **1** to select the file **testbackup.cfg**.

```
Please input the file number to change: 1
```

3. Enter **Y** at the confirmation prompt.

```
The file you selected is testbackup.cfg,Delete it? (Y/N):Y
Deleting.................................Done!
```

Changing the attribute of software images

Software image attributes include main (M), backup (B), and none (N). System software and boot software can each have multiple none-attribute images but only one main image and one backup image on the switch. You can assign both the M and B attributes to one image. If the M or B attribute you are assigning has been assigned to another image, the assignment removes the attribute from that image. If the removed attribute is the sole attribute of the image, its attribute changes to N.

For example, the system image **system.bin** has the M attribute and the system image **system-update.bin** has the B attribute. After you assign the M attribute to **system-update.bin**, the attribute of **system-update.bin** changes to M+B and the attribute of **system.bin** changes to N.

To change the attribute of a system or boot image:

1. Enter **2** in the Boot menu.

```
   EXTENDED BOOT MENU


1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run

Enter your choice(0-8): 2
```

2. **1** or **2** at the prompt to set the attribute of a software image. (The following output is based on the option **2**. To set the attribute of a configuration file, enter **3**.)

```
1. Set image file
2. Set bin file
3. Set configuration file
0. Return to boot menu

Enter your choice(0-3): 2

File Number    File Size(bytes)     File Name
================================================================================

1(*)              53555200              flash:/system.bin
2(*)              9959424               flash:/boot.bin
3                 13105152              flash:/boot-update.bin
4                 91273216              flash:/system-update.bin
Free space: 417177920 bytes
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
Note:Select .bin files. One but only one boot image and system image must be included.
```

3. Enter the number of the file you are working with. For example, enter 3 to select the boot image **boot-update.bin**. And enter **4** to select the system image **system-update.bin**.

```
Enter file No.(Allows multiple selection):3
Enter another file No.(0-Finish choice):4
```

4. Enter **0** to finish the selection.

```
Enter another file No.(0-Finish choice):0
You have selected:
flash:/boot-update.bin
flash:/system-update.bin
```

5. Enter **M** or **B** to change its attribute to main or backup. If you change its attribute to M, the attribute of **boot.bin** changes to none.

```
Please input the file attribute (Main/Backup) M
This operation may take several minutes. Please wait....
Next time, boot-update.bin will become default boot file!
Next time, system-update.bin will become default boot file!
Set the file attribute success!
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version.

To handle a software upgrade failure:

1. Verify that the software release is compatible with the switch model and the correct file is used.
2. Verify that the software release and the Boot ROM release are compatible. For software and Boot ROM compatibility, see the hardware and software compatibility matrix in the correct release notes.
3. Check the physical ports for a loose or incorrect connection.

4. 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.
5. 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.
6. Check the FTP or TFTP server for any incorrect setting.
7. Check that the storage device has sufficient space for the upgrade file.

Hewlett Packard Enterprise

HPE 5510HI-CMW710-R3507 Release Notes Software Feature Changes

Contents

R3507

This release has the following changes:

- Modified feature: EAD assistant

Modified feature: EAD assistant

Feature change description

As from this version, you can use both EAD assistant and MAC authentication on the device.

Before modification: EAD assistant is mutually exclusive with MAC authentication and port security.

- You cannot enable EAD assistant when MAC authentication or port security is enabled globally.
- You cannot enable MAC authentication or port security globally when EAD assistant is enabled.

After modification: EAD assistant is still mutually exclusive with the port security feature, but you can use both EAD assistant and MAC authentication on the device. When you use both EAD assistant and MAC authentication on the device, follow these restrictions and guidelines:

- If both EAD assistant and MAC authentication are configured on the device, the MAC address of a user that fails MAC authentication is not marked as a silent MAC address. If the user has never passed MAC authentication, packets from the user can trigger MAC authentication again only after the user's EAD entry ages out.
- As a best practice, do not configure MAC authentication guest VLANs, guest VSIs, critical VALNs, or critical VSIs. The VLANs or VSIs might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- As a best practice, do not configure the Web authentication or IP source guard feature. The feature might fail to work correctly when both EAD assistant and MAC authentication are configured on the device.
- If the MAC address of a user has been marked as a silent MAC address before EAD assistant is enabled, packets from the user can trigger 802.1X or MAC authentication only after the quiet timer expires.

Command changes

None.

R3506P10

This release has the following changes:

- New feature: Configuring the 802.1p priority for control packets sent by a device
- New feature: Packet spoofing logging and filtering entry logging for SAVI
- New feature: Configuring password control over weak passwords
- New feature: Enabling password change prompt logging
- New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device
- Modified feature: Flow-mirroring traffic to a tunnel interface

New feature: Configuring the 802.1p priority for control packets sent by a device

Configure the 802.1p priority for control packets sent by the device

About this task

By default, the 802.1p priority is 6 for control packets sent by a device. However, some devices will drop or not process packets with 802.1p priority 6, which affects the operation of protocols in the network. To resolve this problem, configure the 802.1p priority for control packets sent by a device.

Restrictions and guidelines

This feature configures the 802.1p priority for packets of the following protocols: ARP, DNS, NTP, OSPF, BGP, PIM, ICMP, SSH, Telnet, LDP, RADIUS, SYSLOG, and SNMP.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the 802.1p priority for control packets sent by the device.	**control-packet dot1p** *priority*	By default, the 802.1p priority is 6 for control packets sent by a device.

Command reference

control-packet dot1p

Use **control-packet dot1p** to configure the 802.1p priority for control packets sent by the device.

Use **undo control-packet dot1p** to restore the default.

Syntax

control-packet dot1p *priority*

undo control-packet dot1p

Default

The 802.1p priority is 6 for control packets sent by a device.

Views

System view

Predefined user roles

network-admin

network-operator

Parameters

priority: Specifies an 802.1p priority value in the range of 0 to 7. 0 indicates the lowest priority, and 7 indicates the highest priority.

Usage guidelines

By default, the 802.1p priority is 6 for control packets sent by a device. However, some devices will drop or not process packets with 802.1p priority 6, which affects the operation of protocols in the network. To resolve this problem, configure the 802.1p priority for control packets sent by a device.

This command configures the 802.1p priority for packets of the following protocols: ARP, DNS, NTP, OSPF, BGP, PIM, ICMP, SSH, Telnet, LDP, RADIUS, SYSLOG, and SNMP. As a best practice, make sure you known the impact before executing this command.

Examples

Configure the 802.1p priority as 7 for control packets sent by the device.

```
<Sysname> system-view
[Sysname] control-packet dot1p 7
```

New feature: Packet spoofing logging and filtering entry logging for SAVI

Enabling packet spoofing logging and filtering entry logging

About this task

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see *Network Management and Monitoring Configuration Guide*.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable packet spoofing logging.	**ipv6 savi log enable spoofing-packet** [**interval** *interval* | **total-number** *number*] *	By default, packet spoofing logging is disabled.
3. Enable filtering entry logging.	**ipv6 savi log enable filter-entry**	By default, filtering entry logging is disabled.

Command reference

ipv6 savi log enable

Use **ipv6 savi log enable** to enable packet spoofing logging or filtering entry logging.

undo ipv6 savi log enable to disable packet spoofing logging or filtering entry logging.

Syntax

ipv6 savi log enable { **spoofing-packet** [**interval** *interval* | **total-number** *number*] * | **filter-entry** }

undo ipv6 savi log enable { **spoofing-packet** | **filter-entry** }

Default

Packet spoofing logging and filtering entry logging are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

spoofing-packet [**interval** *interval* | **total-number** *number*]: Enables packet spoofing logging.

- **interval** *interval*: Sets the log output interval in seconds. The value of the *interval* argument can be 0 or in the range of 5 to 3600. The default value is 60 seconds. If you set this parameter to 0, the device outputs a log message immediately after it is generated.
- **total-number** *number*: Sets the maximum number of log messages that can be output per interval. The value range for the *number* argument is 1 to 128, and the default value is 128.

filter-entry: Enables filtering entry logging.

Usage guidelines

Packet spoofing logging enables the device to generate log messages for the spoofed packets detected by SAVI.

Filtering entries are effective bindings used for filtering IPv6 packets by the source IPv6 address. Filtering entry logging enables the device to generate log messages for filtering entries. A log message contains the IPv6 address, MAC address, VLAN, and interface of a filtering entry.

The device sends packet spoofing and filtering entry log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations. For more information about using the information center, see *Network Management and Monitoring Configuration Guide*.

The device can output a maximum of 128 packet spoofing log messages. If this limit is crossed, the device drops excess log messages. To ensure device performance, set the log output interval and maximum number of log messages output per interval appropriately.

Examples

Enable packet spoofing logging.

```
<Sysname> system-view
[Sysname] ipv6 savi log enable spoofing-packet
```

New feature: Configuring password control over weak passwords

Configuring password control over weak passwords

About this task

The system checks for weak passwords for Telnet or SSH device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.
- Minimum password length restriction.
- Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

Procedure

To enable mandatory weak password change:

Step	Command	Remarks
4. Enter system view.	**system-view**	N/A
5. Enable mandatory weak password change.	**password-control change-password weak-password enable**	By default, the mandatory weak password change feature is disabled.

Command reference

New command: password-control change-password weak-password enable

Use **password-control change-password weak-password enable** to enable mandatory weak password change.

Use **undo password-control change-password weak-password enable** to disable mandatory weak password change.

Syntax

password-control change-password weak-password enable

undo password-control change-password weak-password enable

Default

The mandatory weak password change feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The system checks for weak login passwords for Telnet or SSH device management users. A password is weak if it does not meet the following requirements:

- Password composition restriction.
- Minimum password length restriction.
- Cannot contain the username or the reverse letters of the username.

By default, the system displays a message about a weak password but does not force the user to change it. To improve the device security, you can enable the mandatory weak password change feature, which forces the users to change the identified weak passwords. The users can log in to the device only after their passwords meet the password requirements.

By default, the global composition policy and global minimum password length are as follows:

- A password must contain a minimum of two character types and a minimum of one character for each type.
- A password must contain a minimum of 10 characters.

By default, the password composition policy for a user group equals the global setting. The password composition policy for a local user equals that of the user group to which the local user belongs.

To change the password composition restriction and minimum password length, use the **password-control composition** and **password-control length** commands, respectively.

Examples

Enable the mandatory weak password change feature.

```
<Sysname> system-view
[Sysname] password-control change-password weak-password enable
```

Related commands

password-control { **aging** | **composition** | **history** | **length** } **enable**

password-control complexity

password-control composition

password-control length

password-control enable

Modified command: display password-control

Use **display password-control** to display password control configuration.

Syntax

display password-control [**super**]

Views

Any view

Change description

Before modification: The **Password change** field does not contain the enabling state of the mandatory weak password change feature.

After modification: The **Password change** field displays the enabling state of the mandatory weak password change feature, including **Enabled (mandatory weak password change)** and **Disabled (mandatory weak password change)**.

Modified command: password-control complexity

Use **password-control complexity** to configure the password complexity checking policy.

Use **undo password-control complexity** to remove a password complexity checking item.

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

Views

System view

User group view

Local user view

Change description

Before modification: By default, the global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

After modification: By default, the global password complexity checking policy is as follows:

- In non-FIPS mode:

  The global password complexity checking policy is that username checking is enabled and repeated character checking is disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

- In FIPS mode:

  The global password complexity checking policy is that both username checking and repeated character checking are disabled. The password complexity checking policy for a user group equals the global setting. The password complexity checking policy for a local user equals that of the user group to which the local user belongs.

Modified command: password-control composition

Use **password-control composition** to configure the password composition policy.

Use **undo password-control composition** to restore the default.

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

Views

System view

User group view

Local user view

Change description

Before modification: By default, the global composition policy requires that a password must contain a minimum of one character type and a minimum of one character for each type.

After modification: By default, the global composition policy requires that a password must contain a minimum of two character types and a minimum of one character for each type.

Modified command: password-control super composition

Use **password-control super composition** to configure the composition policy for super passwords.

Use **undo password-control super composition** to restore the default.

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

Views

System view

Change description

Before modification: By default, a super password must contain a minimum of one character type and a minimum of one character for each type.

After modification: By default, a super password must contain a minimum of two character types and a minimum of one character for each type.

Modified command: set authentication password

Use **set authentication password** to set the password for local password authentication.

Use **undo set authentication password** to restore the default.

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Change description

Before modification: The password in plaintext form is a string of 1 to 16 characters.

After modification: The password in plaintext form is a string of 4 to 16 characters, and must contain a minimum of two character types and a minimum of one character for each type.

New feature: Enabling password change prompt logging

Enabling password change prompt logging

About this task

Use this feature to enhance the protection of passwords for Telnet, SSH, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the password-control composition command.
- Minimum password length restriction set by using the password-control length command.
- It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

Restrictions and guidelines

You can use the display password-control command to display password control configuration. For more information about password control commands, see password control commands in *Security Command Reference*.

Procedure

To enable password change prompt logging:

Step	Command	Remarks
6. Enter system view.	**system-view**	N/A
7. Enable recording untrusted DHCP servers.	**local-server log change-password-prompt**	By default, password change prompt logging is enabled.

Command reference

local-server log change-password-prompt

Use local-server log change-password-prompt to enable password change prompt logging.

Use undo local-server log change-password-prompt to disable password change prompt logging.

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

Default

Password change prompt logging is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this feature to enhance the protection of passwords for Telnet, SSH, NETCONF over SSH, and NETCONF over SOAP users and improve the system security.

This feature enables the device to generate logs to prompt users to change their weak passwords at an interval of 24 hours and at the users' login.

A password is a weak password if it does not meet the following requirements:

- Password composition restriction configured by using the password-control composition command.
- Minimum password length restriction set by using the password-control length command.
- It cannot contain the username or the reverse letters of the username.

For a NETCONF over SSH or NETCONF over SOAP user, the device also generates a password change prompt log if any of the following conditions exists:

- The current password of the user is the default password or has expired.
- The user logs in to the device for the first time or uses a new password to log in after global password control is enabled.

The device will no longer generate password change prompt logs for a user when one of the following conditions exists:

- The password change prompt logging feature is disabled.
- The user has changed the password and the new password meets the password control requirements.
- The enabling status of a related password control feature has changed so the current password of the user meets the password control requirements.
- The password composition policy or the minimum password length has changed.

You can use the display password-control command to display password control configuration. For more information about password control commands, see password control commands in *Security Command Reference*.

Examples

Enable password change prompt logging.

```
<Sysname> system-view
[Sysname] local-server log change-password-prompt
```

Related commands

display password-control

password-control composition

password-control length

New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device

Enabling recording untrusted DHCP servers on a DHCP snooping device

About this task

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With

feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Procedure

1. Enter system view.
   `system-view`
2. Enable recording untrusted DHCP servers.
   `dhcp snooping untrusted-server-record enable`
   By default, the device does not record untrusted DHCP servers.

Command reference

dhcp snooping untrusted-server-record enable

Use **`dhcp snooping untrusted-server-record enable`** to enable recording untrusted DHCP servers.

Use **`undo dhcp snooping untrusted-server-record enable`** to disable recording untrusted DHCP servers.

Syntax

`dhcp snooping untrusted-server-record enable`

`undo dhcp snooping untrusted-server-record enable`

Default

Recording untrusted DHCP servers is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Examples

Enable the DHCP snooping device to record untrusted DHCP servers

```
<Sysname> system-view
[Sysname] dhcp snooping untrusted-server-record enable
```

Modified feature: Flow-mirroring traffic to a tunnel interface

Feature change description

From this release, traffic can be mirrored to a tunnel interface through flow mirroring.

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*] *]

New syntax

Syntax 1:

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*

Syntax 2:

mirror-to interface 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 destination-ip *destination-ip-address* **source-ip** *source-ip-address*

Views

Traffic behavior view

Change description

Before modification: This command does not support the **destination-mac** keyword of syntax 1 and does not support syntax 2.

After modification: This command supports the **destination-mac** keyword of syntax 1 and supports syntax 2.

*interface-type interface-numbe*r: Specifies an interface by its type and number.

destination-ip *destination-ip-address*: Specifies the destination IP address for the mirrored packets.

source-ip *source-ip-address*: Specifies the source IP address for the mirrored packets.

dscp *dscp-value*: Specifies the DSCP value for the mirrored packets. The *dscp-value* argument can be a number in the range of 0 to 63 or a keyword in Table 1.

Table 1 DSCP keywords and values

Keyword	DSCP value in binary	DSCP value in decimal
af11	001010	10
af12	001100	12

Keyword	DSCP value in binary	DSCP value in decimal
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094 for the mirrored packets.

vrf-instance *vrf-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The mirrored packets will be forwarded based on the routing table of the specified VPN instance.

destination-mac *mac-address*: Specifies the destination MAC address for mirrored packets sent to the interface. The *mac-address* argument is in the format of H-H-H. If you do not specify this option, the device uses the destination IP address to dynamically get the destination MAC address for the mirrored packets.

Release 3506P08

This release has no feature changes.

Release 3506P06

This release has the following changes:

- New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device
- Modified feature: Flow-mirroring traffic to a tunnel interface
- Modified feature: Factory defaults change for console login and password control settings

New feature: Enabling recording untrusted DHCP servers on a DHCP snooping device

Enabling recording untrusted DHCP servers on a DHCP snooping device

About this task

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Procedure

To enable recording untrusted DHCP servers on a DHCP snooping device:

Step	Command	Remarks
8. Enter system view.	**system-view**	N/A
9. Enable recording untrusted DHCP servers.	**dhcp snooping untrusted-server-record enable**	By default, the device does not record untrusted DHCP servers.

Command reference

dhcp snooping untrusted-server-record enable

Use dhcp snooping untrusted-server-record enable to enable recording untrusted DHCP servers.

Use undo dhcp snooping untrusted-server-record enable to disable recording untrusted DHCP servers.

Syntax

dhcp snooping untrusted-server-record enable

undo dhcp snooping untrusted-server-record enable

Default

Recording untrusted DHCP servers is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Typically, a DHCP snooping device identifies the DHCP servers that are connected to the untrusted ports as untrusted. The snooping device drops incoming DHCP replies through these ports. With feature enabled, the snooping device will record the DHCP servers for dropped DHCP replies, and generate and send log messages to the information center. With the information center, you can set log message filtering and output rules, including output destinations.

This command takes effect after DHCP snooping is enabled in a VLAN. If DHCP snooping is enabled globally or in a VXLAN, this command does not take effect.

If a log message is generated for an untrusted DHCP server, no more log messages will be generated for this server within 10 minutes. When the 10-minute interval expires, the DHCP snooping device will generate a log message for this server upon receiving a reply from this server.

Examples

Enable the DHCP snooping device to record untrusted DHCP servers

```
<Sysname> system-view
[Sysname] dhcp snooping untrusted-server-record enable
```

Modified feature: Flow-mirroring traffic to a tunnel interface

Feature change description

From this release, traffic can be mirrored to a tunnel interface through flow mirroring.

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*] *]

New syntax

Syntax 1:

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*

Syntax 2:

mirror-to interface 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 destination-ip *destination-ip-address* **source-ip** *source-ip-address*

Views

Traffic behavior view

Change description

Before modification: This command does not support the **destination-mac** keyword of syntax 1 and does not support syntax 2.

After modification: This command supports the **destination-mac** keyword of syntax 1 and supports syntax 2.

*interface-type interface-numbe*r: Specifies an interface by its type and number.

destination-ip *destination-ip-address*: Specifies the destination IP address for the mirrored packets.

source-ip *source-ip-address*: Specifies the source IP address for the mirrored packets.

dscp *dscp-value*: Specifies the DSCP value for the mirrored packets. The *dscp-value* argument can be a number in the range of 0 to 63 or a keyword in Table 1.

Table 2 DSCP keywords and values

Keyword	DSCP value in binary	DSCP value in decimal
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	000000	0
ef	101110	46

vlan *vlan-id*: Specifies a VLAN by its VLAN ID in the range of 1 to 4094 for the mirrored packets.

vrf-instance *vrf-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters. The mirrored packets will be forwarded based on the routing table of the specified VPN instance.

destination-mac *mac-address*: Specifies the destination MAC address for mirrored packets sent to the interface. The *mac-address* argument is in the format of H-H-H. If you do not specify this option, the device uses the destination IP address to dynamically get the destination MAC address for the mirrored packets.

Modified feature: Factory defaults change for console login and password control settings

Feature change description

Factory defaults are custom basic settings that came with the device. You can use the **display default-configuration** command to display factory defaults.

The device starts up with the factory defaults if no next-startup configuration files are available.

In this version, the following factory default settings are added:

```
#
password-control enable
#
local-user admin class manage
service-type terminal
authorization-attribute user-role network-admin
#
line class aux
authentication-mode scheme
#
undo password-control aging enable
#
undo password-control composition enable
#
undo password-control history enable
#
undo password-control length enable
#
password-control login idle-time 0
#
password-control login-attempt 3 exceed unlock
#
password-control update-interval 0
#
```

The output shows that the factory defaults for console login and password control settings change:

- The device performs local AAA authentication for console users. A console user must use the username **admin** without any password to log in to the device for the first time. The user role **network-admin** is assigned to the login console user.
- By default, the global password control and password change at first login are both enabled. Users must change the password at first login before they can access the system. The new password must contain a minimum of four different characters.

- The default maximum account idle time is 0 days. The system has no restriction for the account idle time.
- The default minimum password update interval is 0 hours. The system has no requirement for the password update interval.
- The default maximum number of consecutive login failures is 3. When console user fails the maximum number of login attempts, the console user can continue using this user account to make login attempts.
- After a console user modifies the password after first login, if you want to delete the default user account **admin**, make sure either of the following conditions are met before deleting the user account **admin**:
  - Another user account with the highest permissions exists.
  - The **authentication-mode none** command has been configured for AUX user lines.
- If you add or modify security configurations, make sure they do not conflict with the factory defaults or will not lead login failures. For more information about factory defaults, see configuration file management in *Fundamentals Configuration Guide* for the product. For more information about AAA authentication and password control, see *Security Configuration Guide.*
- After the global password control is enabled, the device generates an lauth.dat file to save the authentication and login information for local users.
  - If you execute the **restore factory-default** command in user view to restore the factory defaults, the lauth.dat file will be deleted. After the device reboots, you can use the username **admin** without any password to log in to the device, and you are required to change the password.
  - If you restore the factory defaults through **Restore to factory default configuration** on the boot menu, the lauth.dat file will not be deleted. After the device reboots, you must use the latest password to log in to the device.

Command changes

None.

Release 3506P03

This release has no feature changes.

Release 3506P02

This release has no feature changes.

Release 3506P01

This release has no feature changes.

Release 3506

This chapter includes following contents:

New feature: Associating Track with a tracked list

Associating Track with a tracked list

Associating Track with a Boolean list

About this task

A Boolean list is a list of tracked objects based on a Boolean logic. It can be further divided into the following types:

- **Boolean AND list**—When all objects in the list are in Positive state, the Track module sets the track entry to Positive state. When one or more objects are in Negative state, the Track module sets the track entry to Negative state.
- **Boolean OR list**—When any object is in Positive state, the Track module sets the track entry to Positive state. When all objects are in Negative state, the Track module sets the track entry to Negative state.

Procedure

To associate Track with a Boolean list:

Step	Command	Remarks
10. Enter system view.	**system-view**	N/A
11. Create a track entry associated with a Boolean list, and enter Track view.	**track** *track-entry-number* **list boolean** { **and** | **or** }	N/A
12. Set the delay for notifying the application module of track entry state changes.	**delay** { **negative** *negative-time* | **positive** *positive-time* } *	By default, the Track module notifies the application module immediately when the track entry state changes.
13. Add a track entry as an object to the tracked list.	**object** *track-entry-number* [**not**]	By default, a tracked list does not contain any objects.

Associating Track with a percentage threshold list

About this task

The Track module determines the state of a track entry associated with a percentage threshold list as follows:

- If the percentage of Positive objects in the list is equal to or above the positive state threshold, the Track module sets the track entry to Positive state.
- If the percentage of Positive objects in the list is equal to or below the negative state threshold, the Track module sets the track entry to Negative state.
- The track entry state remains unchanged if the percentage of Positive objects in the list is below the positive state threshold and above the negative state threshold.

Procedure

To associate Track with a percentage threshold list:

Step	Command	Remarks
14. Enter system view.	**system-view**	N/A
15. Create a track entry associated with a percentage threshold list, and enter Track view.	**track** *track-entry-number* **list threshold percentage**	N/A
16. Set the delay for notifying the application module of track entry state changes.	**delay** { **negative** *negative-time* | **positive** *positive-time* } *	By default, the Track module notifies the application module immediately when the track entry state changes.
17. Add a track entry as an object to the tracked list.	**object** *track-entry-number*	By default, a tracked list does not contain any objects.
18. Configure the threshold values used to determine the state of the percentage threshold list.	**threshold percentage** { **negative** *negative-threshold* | **positive** *positive-threshold* } *	By default, the negative state threshold is 0% and the positive state threshold is 1%.

Associating Track with a weight threshold list

About this task

The Track module determines the state of a track entry associated with a weight threshold list as follows:

- If the total weight of Positive objects in the list is equal to or above the positive state threshold, the Track module sets the track entry to Positive state.
- If the total weight of Positive objects in the list is equal to or below the negative state threshold, the Track module sets the track entry to Negative state.
- The track entry state remains unchanged if the total weight of Positive objects in the list is below the positive state threshold and above the negative state threshold.

Procedure

To associate Track with a weight threshold list:

Step	Command	Remarks
19. Enter system view.	**system-view**	N/A
20. Create a track entry	**track** *track-entry-number* **list**	N/A

Step	Command	Remarks
associated with a weight threshold list, and enter Track view.	**threshold weight**	
21. Set the delay for notifying the application module of track entry state changes.	**delay** { **negative** *negative-time* | **positive** *positive-time* } *	By default, the Track module notifies the application module immediately when the track entry state changes.
22. Add a track entry as an object to the tracked list.	**object** *track-entry-number* [**weight** *weight*]	By default, a tracked list does not contain any objects.
23. Configure the threshold values used to determine the state of the weight threshold list.	**threshold weight** { **negative** *negative-threshold* | **positive** *positive-threshold* } *	By default, the negative state threshold is 0 and the positive state threshold is 1.

Command reference

object

Use **object** to add a track entry as an object to a tracked list.

Use **undo object** to remove the object from a tracked list

Syntax

object *track-entry-number* [**not**] [**weight** *weight*]

undo object *track-entry-number*

Default

A tracked list does not contain any objects.

Views

Track view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies a track entry by its ID in the range of 1 to 1024.

not: Negates the state of the object. For example, the tracked list determines the object to be Negative when the object is in Positive state. This keyword is supported only by a Boolean list.

weight *weight*: Assigns a weight in the range of 1 to 255 to the object. This keyword is supported only by a weight threshold list. The default weight is 10.

Usage guidelines

The track entry ID of the object cannot be the same as the ID of the tracked list to which the object is added.

You can add a maximum of 16 objects to a tracked list.

Loops are not allowed between track entries. For example, after you add track entry 1 (object 1) to tracked list 2 and track entry 2 (object 2) to tracked list 3, you cannot add track entry 3 (object 3) to tracked list 1 because a loop will be created.

Examples

Create Boolean AND list 100 and add track entries 1 and 2 as tracked objects to the list.

```
<Sysname> system-view
[Sysname] track 100 list boolean and
[Sysname-track-100] object 1
[Sysname-track-100] object 2 not
```

Related commands

track list boolean

track list threshold percentage

track list threshold weight

threshold percentage

Use **threshold percentage** to set the threshold values for a percentage threshold list.

Use **undo threshold percentage** to restore the default.

Syntax

threshold percentage { **negative** *negative-threshold* | **positive** *positive-threshold* } *

undo threshold percentage

Default

The negative state threshold is 0% and the positive state threshold is 1%.

Views

Track view

Predefined user roles

network-admin

Parameters

negative *negative-threshold*: Specifies the negative state threshold in the range of 0 to 100. For the track entry to be set to the Negative state, the percentage of Positive objects must be equal to or smaller than the configured negative state threshold.

positive *positive-threshold*: Specifies the positive state threshold in the range of 0 to 100. For the track entry to be set to the Positive state, the percentage of Positive objects must be equal to or greater than the configured positive state threshold. The *positive-threshold* must be greater than the *negative-threshold*.

Usage guidelines

The track entry state remains unchanged if the percentage of Positive objects is below the positive state threshold and above the negative state threshold.

This command is supported only by a track entry associated with a percentage threshold list.

Examples

Set the negative state threshold to 30% and the positive state threshold to 50% for track entry 1 associated with a percentage threshold list.

```
<Sysname> system-view
[Sysname] track 1 list threshold percentage
[Sysname-track-1] threshold percentage negative 30 positive 50
```

Related commands

track list threshold percentage

threshold weight

Use **threshold weight** to set the threshold values for a weight threshold list.

Use **undo threshold weight** to restore the default.

Syntax

threshold weight { **negative** *negative-threshold* | **positive** *positive-threshold* } *

undo threshold weight

Default

The negative state threshold is 0 and the positive state threshold is 1.

Views

Track view

Predefined user roles

network-admin

Parameters

negative *negative-threshold*: Specifies the negative state threshold in the range of 0 to 254. For the track entry to be set to the Negative state, the total weight of Positive objects must be equal to or smaller than the configured negative state threshold.

positive *positive-threshold*: Specifies the positive state threshold in the range of 1 to 255. For the track entry to be set to the Positive state, the total weight of Positive objects must be equal to or greater than the configured positive state threshold. The *positive-threshold* must be greater than the *negative-threshold*.

Usage guidelines

The track entry state remains unchanged if the total weight of Positive objects is below the positive state threshold and above the negative state threshold.

This command is supported only by a track entry associated with a weight threshold list.

Examples

Set the negative state threshold to 30 and the positive state threshold to 50 for track entry 1 associated with a weight threshold list.

```
<Sysname> system-view
[Sysname] track 1 list threshold weight
[Sysname-track-1] threshold weight negative 30 positive 50
```

Related commands

track list threshold weight

track list boolean

Use **track list boolean** to create a track entry associated with a Boolean list and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **list boolean** { **and** | **or** }

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

and: Associates the track entry with a Boolean AND list.

or: Associates the track entry with a Boolean OR list.

Usage guidelines

A Boolean list is a list of tracked objects based on a Boolean logic. It can be further divided into the following types:

- **Boolean AND list**—When all objects in the list are in Positive state, the Track module sets the track entry to Positive state. When one or more objects are in Negative state, the Track module sets the track entry to Negative state.
- **Boolean OR list**—When any object is in Positive state, the Track module sets the track entry to Positive state. When all objects are in Negative state, the Track module sets the track entry to Negative state.

To create a track entry, you must specify the tracked object type, which is **list boolean** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track list boolean** command again.

Examples

Create track entry 101 and associate it with a Boolean OR list.

```
<Sysname> system-view
[Sysname] track 101 list boolean or
[Sysname-track-101]
```

Related commands

delay

object

track list threshold percentage

Use **track list threshold percentage** to create a track entry associated with a percentage threshold list and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **list threshold percentage**

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

Usage guidelines

The Track module determines the state of a track entry by comparing the percentage of Positive objects in the list with the percentage thresholds configured for the list. To configure the threshold values used to determine the track entry state, use the **threshold percentage** command.

To create a track entry, you must specify the tracked object type, which is **list threshold percentage** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings of a track entry, execute the **undo track** command to remove the track entry, and then execute the **track list threshold percentage** command again.

Examples

Create track entry 101 and associate it with a percentage threshold list.

```
<Sysname> system-view
[Sysname] track 101 list threshold percentage
[Sysname-track-101]
```

Related commands

delay

object

threshold percentage

track list threshold weight

Use **track list threshold weight** to create a track entry associated with a weight threshold list and enter Track view, or enter the view of an existing track entry.

Use **undo track** to remove the track entry and all its settings.

Syntax

track *track-entry-number* **list threshold weight**

undo track *track-entry-number*

Default

No track entries exist.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

Usage guidelines

The Track module determines the state of a track entry by comparing the weight of Positive objects in the list with the weight thresholds configured for the list. To configure the threshold values used to determine the track entry state, use the **threshold weight** command.

To create a track entry, you must specify the tracked object type, which is **list threshold weight** in this command.

To enter the view of an existing track entry, use the **track** *track-entry-number* command. The tracked object type is not required.

To modify the settings for a track entry, execute the **undo track** command to remove the track entry, and then execute the **track list threshold weight** command again.

Examples

Create track entry 101 and associate it with a weight threshold list.

```
<Sysname> system-view
[Sysname] track 101 list threshold weight
[Sysname-track-101]
```

Related commands

delay

object

threshold weight

New feature: LDRA on the DHCPv6 snooping device

Enabling LDRA on the DHCPv6 snooping device

About LDRA on the DHCPv6 snooping device

Some DHCPv6 servers assign IPv6 addresses or prefixes to DHCPv6 clients only based on the Interface ID option in a Relay-Forward packet. If no DHCPv6 relay agent exists between DHCPv6 clients and such a DHCP server, the IPv6 address or prefix assignment based on the Interface ID option will fail.

To solve this problem, you can enable the lightweight DHCPv6 relay agent (LDRA) on the interface that receives DHCPv6 requests. The feature allows the interface to generate a Relay-Forward packet for a received DHCPv6 request and to insert the Interface ID option in the packet. After receiving the Relay-Forward packet, the DHCPv6 server can assign an IPv6 address or prefix based on the Interface ID option.

Procedure

To enable LDRA on an interface:

Step	Command	Remarks
24. Enter system view.	**system-view**	N/A
25. Enter interface view.	**interface** *interface-type interface-number*	N/A
26. Enable LDRA on the interface.	**ipv6 dhcp snooping relay-agent enable**	By default, LDRA is disabled on the interface.

Command reference

ipv6 dhcp snooping relay-agent enable

Use **ipv6 dhcp snooping relay-agent enable** to enable LDRA on an interface.

Use **undo ipv6 dhcp snooping relay-agent enable** to disable LDRA on an interface.

Syntax

ipv6 dhcp snooping relay-agent enable [**trust**]

undo ipv6 dhcp snooping relay-agent enable [**trust**]

Default

By default, LDRA is disabled on the interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

trust: Specifies the interface as a trusted interface. The device trusts the Relay-Forward packets received on the interface and forwards these packets to the DHCPv6 server. If you do not specify this keyword, the device drops the Relay-Forward packets received on this interface.

Usage guidelines

A network might have multiple cascaded lightweight DHCPv6 relay agents. As a best practice, do not specify the **trust** keyword if illegal Relay-Forward packets exist in the network.

Before you enable this feature, execute the **ipv6 dhcp snooping enable** command to enable DHCPv6 snooping. Otherwise, this feature does not take effect.

If this command and the **ipv6 dhcp snooping option interface-id enable** command are both executed, this command does not take effect.

Examples

Enable LDRA on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping relay-agent enable
```

New feature: Controlling the status of guest VLAN reauthentication in MAC authentication

Enabling guest VLAN reauthentication in MAC authentication

Overview

The guest VLAN reauthentication feature of MAC authentication enables the device to reauthenticate users in the MAC authentication guest VLAN on a port at reauthentication intervals.

In software versions earlier than R3503, guest VLAN reauthentication is enabled by default and cannot be disabled from the CLI.

As from version R3503, you can enable guest VLAN reauthentication by using the **mac-authentication guest-vlan re-authenticate** command or disable the feature by using the **undo** form of the command.

Typically, you disable this feature to suppress excessive authentication failure log messages, which might occur when a network issue results in a large number of reauthentication failures.

If guest VLAN reauthentication is disabled on a port, the device does not reauthenticate users in the MAC authentication guest VLAN on the port. The guest VLAN users will stay in the guest VLAN until they age out. To configure the aging timer, use the **mac-authentication timer user-aging guest-vlan** *aging-time-value* command.

As a best practice, set the reauthentication interval to a value greater than 30 seconds if the number of concurrent MAC authentication users on a port is likely to exceed 300.

Configuration procedure

To enable the guest VLAN reauthentication feature of MAC authentication on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the guest VLAN reauthentication feature of MAC authentication on the port.	**mac-authentication guest-vlan re-authenticate**	By default, the guest VLAN reauthentication feature of MAC authentication is enabled on a port.

Command reference

mac-authentication guest-vlan re-authenticate

Use **mac-authentication guest-vlan re-authenticate** to enable the guest VLAN reauthentication feature of MAC authentication on a port.

Use **undo mac-authentication guest-vlan re-authenticate** to disable the guest VLAN reauthentication feature of MAC authentication on a port.

Syntax

mac-authentication guest-vlan re-authenticate

undo mac-authentication guest-vlan re-authenticate

Default

The guest VLAN reauthentication feature of MAC authentication is enabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The guest VLAN reauthentication feature of MAC authentication enables the device to reauthenticate users in the MAC authentication guest VLAN on a port at reauthentication intervals.

Typically, you disable this feature to suppress excessive authentication failure log messages, which might occur when a network issue results in a large number of reauthentication failures.

If guest VLAN reauthentication is disabled on a port, the device does not reauthenticate users in the MAC authentication guest VLAN on the port. The guest VLAN users will stay in the guest VLAN until they age out. To configure the aging timer, use the **mac-authentication timer user-aging guest-vlan** *aging-time-value* command.

Examples

Enable the guest VLAN reauthentication feature of MAC authentication on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan re-authenticate
```

Related commands

display mac-authentication

mac-authentication guest-vlan

mac-authentication guest-vlan auth-period

mac-authentication timer

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

Enabling the DHCPv6 relay agent to support Option 79

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.

To enable the DHCPv6 relay agent to support Option 79:

Step	Command	Remarks
4. Enter system view.	**system-view**	N/A
5. Enter interface view.	**interface** *interface-type interface-number*	N/A
6. 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

ipv6 dhcp relay client-link-address enable

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 vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay client-link-address enable
```

New feature: Zero-to-two VLAN mapping

Configuring zero-to-two VLAN mapping

Overview

Zero-to-two VLAN mappings add double VLAN tags to untagged packets.

Configuration restrictions and guidelines

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.

Configuration procedure

To configure zero-to-two VLAN mapping:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view:	N/A

		interface bridge-aggregation *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.	Set the port PVID to VLAN 1.	• Set the PVID to VLAN 1 for the trunk port: **port trunk pvid vlan 1** • Set the PVID to VLAN 1 for the hybrid port: **port hybrid pvid vlan 1**	N/A
5.	Assign the port to the SVLAN and the port PVID (VLAN 1).	• Assign the trunk port to the SVLAN and the port PVID (VLAN 1): **port trunk permit vlan** *vlan-id-list* • Assign the hybrid port to the SVLAN and the port PVID (VLAN 1) as a tagged member: **port hybrid vlan** *vlan-id-list* **tagged**	By default: • A trunk port is assigned to VLAN 1. • A hybrid port is an untagged member of the VLAN to which the port belongs when its link type is **access**. The SVLAN of the trunk port must be different from the port PVID (VLAN 1).
6.	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.

Command reference

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

Layer 2 Ethernet interface view

Layer 2 aggregate 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 GigabitEthernet 1/0/1 to add SVLAN 200 and CVLAN 100 to untagged packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan mapping untagged nested-outer-vlan 200
nested-inner-vlan 100
```

Related commands

display vlan mapping

New feature: Hash offset configuration for adjusting the load balancing results on aggregate links

Setting a hash offset to adjust the load balancing results on aggregate links

Overview

If undesirable traffic imbalance occurs on aggregate links, you can perform this task to adjust the load sharing results on aggregate links.

Configuration restrictions and guidelines

Misuse of this feature causes unbalanced traffic distribution. Make sure you are fully aware of the impacts of this feature when you configure it on a live network.

Configuration procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set a hash offset to adjust the load sharing results on aggregate links.	**link-aggregation global load-sharing offset** *offset-value*	The default hash offset is 0.

Command reference

link-aggregation global load-sharing offset

Use **link-aggregation global load-sharing offset** to set a hash offset to adjust the load balancing hash results on aggregate links.

Use **undo link-aggregation global load-sharing offset** to restore the default.

Syntax

link-aggregation global load-sharing offset *offset-value*

undo link-aggregation global load-sharing offset

Default

The default hash offset is 0.

Views

System view

Predefined user roles

network-admin

Parameters

offset-value: Specifies a hash offset in the range of 0 to 63.

Usage guidelines

IMPORTANT:

Misuse of this command causes unbalanced traffic distribution. Make sure you are fully aware of the impacts of this command when you execute it on a live network.

If undesirable traffic imbalance occurs on aggregate links, you can use this command to adjust the load sharing results on aggregate links.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the hash offset to 2 for the load balancing hash results on aggregate links.

```
<Sysname> system
[Sysname] link-aggregation global load-sharing offset 2
```

New feature: Load sharing mode for tunneled traffic on aggregate links

Setting the load sharing mode for tunneled traffic

Overview

Perform this task to set the criterion used by aggregation groups to distribute tunneled traffic for load sharing.

The device can use one of the following modes to distribute tunneled traffic on an aggregate link:

- **Inner**—Distributes tunneled traffic based on the inner IP header.
- **Outer**—Distributes tunneled traffic based on the outer IP header.

Configuration procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the load sharing mode for tunneled traffic on aggregate links.	**link-aggregation global load-sharing tunnel** { **inner** | **outer** }	By default, the load sharing mode for tunneled traffic is not configured.

Command reference

link-aggregation global load-sharing tunnel

Use **link-aggregation global load-sharing tunnel** to set the load sharing mode for tunneled traffic on aggregate links.

Use **undo link-aggregation global load-sharing tunnel** to restore the default.

Syntax

link-aggregation global load-sharing tunnel { **inner** | **outer** }

undo link-aggregation global load-sharing tunnel

Default

The load sharing mode for tunneled traffic is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

inner: Distributes tunneled traffic based on the inner IP header.

outer: Distributes tunneled traffic based on the outer IP header.

Usage guidelines

This command sets the criterion used by aggregation groups to distribute tunneled traffic for load sharing.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the load sharing mode to inner IP header for tunneled traffic on aggregate links.

```
<Sysname> system
[Sysname] link-aggregation global load-sharing tunnel inner
```

New feature: Configuring the detection mode of the PD power class

Configuring the detection mode of the PD power class

About the detection mode of the PD power class

A PD is assigned a class from 0 to 4, depending on how much power it requires. The device can automatically detect the power class of its PDs.

- When the device detects power class of 0, 1, 2, or 3, it supplies power based on the detected power class.
- When the device detects power class of 4, it supplies power to the PD based on the configured power class detection mode.
  - **single**—Supplies power to the PD as it is a class 0 device.

- **secondary**—Performs another power class detection and then supplies power based on the second-detected power class.

Procedure

To configure the detection mode of the PD power class:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PI view.	**interface** *interface-type interface-number*	N/A
3. Configure the detection mode of the PD power class.	**poe class-detect** { **single** | **secondary** }	By default, the device uses the secondary mode to detect the PD power class.

Command reference

poe class-detect

Use **poe class-detect** to configure the detection mode of the PD power class.

Use **undo poe class-detect** to restore the default.

Syntax

poe class-detect { **single** | **secondary** }

undo poe class-detect

Default

The device uses the secondary mode to detect the PD power class.

Views

PI view

Predefined user roles

network-admin

Parameters

single: Supplies power to a PD the power class of which is detected 4 as it is a class 0 device.

secondary: Performs another power class detection upon detection of power class 4 and then supplies power based on the second-detected power class.

Usage guidelines

A PD is assigned a class from 0 to 4, depending on how much power it requires. The device can automatically detect the power class of its PDs.

- When the device detects power class of 0, 1, 2, or 3, it supplies power based on the detected power class.
- When the device detects power class of 4, it supplies power to the PD based on the configured power class detection mode:
  - **single**—Supplies power to the PD as it is a class 0 device.
  - **secondary**—Performs another power class detection and then supplies power based on the second-detected power classes.

Examples

Specify the single mode to detect the PD power class on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe classification single
```

New feature: Setting the DSCP value for SNMP response packets

Setting the DSCP value for SNMP response packets

To set the DSCP value for SNMP response packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. (Optional.) Set the DSCP value for SNMP response packets.	**snmp-agent packet response dscp** *dscp-value*	By default, the DSCP value for SNMP response packets is 0.
3. Configure an SNMP trap target host	• In non-FIPS mode: **snmp-agent target-host trap address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]] • In FIPS mode: **snmp-agent target-host trap address udp-domain** { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }	By default, no trap target host is configured.

Command reference

snmp-agent packet response dscp

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP response packets.

Use **undo snmp-agent packet response dscp** to restore the default.

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

Default

The DSCP value for SNMP response packets is 0.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Sets the DSCP value for SNMP response packets, in the range of 0 to 63. A greater DSCP value represents a higher priority.

Usage guidelines

The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet for transmission.

Examples

Set the DSCP value to 40 for SNMP response packets.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 40
```

Modified command: snmp-agent target-host

Old syntax

In non-FIPs mode:

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

In FIPs mode:

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

New syntax

In non-FIPs mode:

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

In FIPs mode:

snmp-agent target-host trap address udp-domain { *ipv4-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] [**dscp** *dscp-value*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* **v3** { **authentication** | **privacy** }

Views

System view

Change description

The **dscp** *dscp-value* option was added to this command.

dscp *dscp-value*: Sets the DSCP value for SNMP response packets, in the range of 0 to 63. The default value is 0. A greater DSCP value represents a higher priority. The DSCP value is encapsulated in the ToS field of an IP packet. It specifies the priority level of the packet for transmission.

New feature: Support for matching SNMP packets in a QoS match criterion

Step	Command	Remarks
4. Enter system view.	**system-view**	N/A
5. Create a traffic class and enter its view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic classes exist.
6. Configure a match criterion for matching SNMP packets.	**if-match control-plane protocol snmp**	By default, no match criterion is configured.

Command reference

if-match control-plane protocol snmp

Use **if-match control-plane protocol snmp** to configure a match criterion for matching SNMP packets.

Use **undo if-match control-plane protocol snmp** to delete an SNMP packet match criterion.

Syntax

if-match control-plane protocol snmp

undo if-match control-plane protocol snmp

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Usage guidelines

A QoS policy that contains the **control-plane protocol** or **control-plane protocol-group** can only be applied to a control plane.

For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Examples

Define a match criterion for traffic class **class1** to match SNMP packets.

```
<Sysname> system
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane snmp
```

New feature: Specifying a MAC address as the IRF bridge MAC address

Specifying a MAC address as the IRF bridge MAC address

CAUTION:
Bridge MAC address change will cause transient traffic disruption.

The bridge MAC address of a system must be unique on a switched LAN. IRF bridge MAC address identifies an IRF fabric by Layer 2 protocols (for example, LACP) on a switched LAN.

By default, an IRF fabric uses the bridge MAC address of the master as the IRF bridge MAC address. After the master leaves, the IRF bridge MAC address persists for a period of time or permanently depending on the IRF bridge MAC persistence setting. When the IRF bridge MAC persistence timer expires, the IRF fabric uses the bridge MAC address of the current master as the IRF bridge MAC address.

In special occasions that require a fixed special IRF bridge MAC address, you can specify that MAC address as the IRF bridge MAC address. For example, before you replace an IRF fabric entirely, you can configure the new IRF fabric with the IRF bridge MAC address of the existing IRF fabric to minimize service interruption.

The IRF bridge MAC persistence setting does not take effect on the manually specified IRF bridge MAC address.

The following is how IRF handles the IRF bridge MAC address if IRF fabrics merge:

- When IRF fabrics merge, IRF ignores the IRF bridge MAC address and checks the bridge MAC address of each member device in the IRF fabrics. IRF merge fails if any two member devices have the same bridge MAC address.
- After IRF fabrics merge, the merged IRF fabric uses the bridge MAC address of the merging IRF fabric that won the master election as the IRF bridge MAC address.

To specify a MAC address as the IRF bridge MAC address:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a MAC address as the IRF bridge MAC address.	**irf mac-address** *mac-address*	By default, an IRF fabric uses the bridge MAC address of the master as the IRF bridge MAC address. If an IRF fabric splits after you configure the IRF bridge MAC address, both the split IRF fabrics use the configured bridge MAC address as the IRF bridge MAC address.

Command reference

irf mac-address

Use **irf mac-address** to specify a MAC address as the IRF bridge MAC address.

Use **undo irf mac-address** to restore the default.

Syntax

irf mac-address *mac-address*

undo irf mac-address

Default

An IRF fabric uses the bridge MAC address of the master device as the IRF bridge MAC address.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H. The MAC address cannot be the all-zero or all-F MAC address, or a multicast MAC address. You can omit the consecutive zeros at the beginning of each segment. For example, you can enter **f-e2-1** for 000f-00e2-0001.

Examples

Configure the IRF fabric to use **c4ca-d9e0-8c3c** as the IRF bridge MAC address.

```
<Sysname> system-view
[Sysname] irf mac-address c4ca-d9e0-8c3c
```

New feature: Multicast VPN

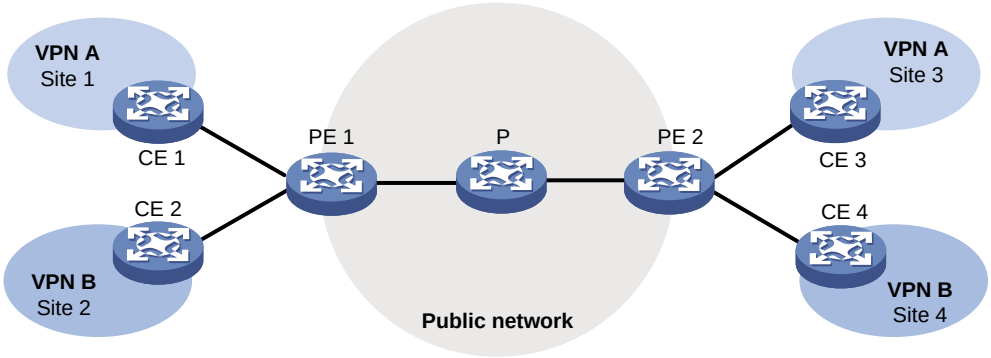
Multicast VPN overview

Multicast VPN implements multicast delivery in VPNs. It ensures that multicast data from a multicast source in a VPN instance is sent only to multicast receivers in the same VPN instance.

Typical network diagram

As shown in Figure 1, VPN A contains Site 1 and Site 3, and VPN B contains Site 2 and Site 4.

Figure 1 Typical network diagram for multicast VPN



VPN multicast traffic between the PEs and the CEs is transmitted on a per-VPN-instance basis. The public network multicast traffic between the PEs and the P device is transmitted through the public network. Multicast VPN provides independent multicast services for the public network, VPN A, and VPN B.

For more information about CEs, PEs and Ps, see *MPLS Configuration Guide*.

MVPN scheme

MVPN is used to implement multicast VPN. MVPN only requires the PEs to support multiple VPN instances and the public network provided by the service provider to support multicast. There is no need to upgrade CEs and Ps or change their PIM configurations. The MVPN solution is transparent to CEs and Ps.

Basic concepts in MDT-based MVPN

This section introduces the following basic concepts in MDT-based MVPN:

- **MVPN**—An MVPN logically defines the transmission boundary of the multicast traffic of a VPN over the public network. It also physically identifies all the PEs that support that VPN instance on the public network. Different VPN instances correspond to different MVPNs.
- **Multicast distribution tree (MDT)**—An MDT is a multicast distribution tree constructed by all PEs in the same VPN. MDT includes default MDT and data MDT.
- **Multicast tunnel (MT)**—An MT is a tunnel that interconnects all PEs in an MVPN. The local PE encapsulates a VPN multicast packet into a public network multicast packet and forwards it through the MT over the public network. The remote PE decapsulates the public network multicast packet to get the original VPN multicast packet.
- **Multicast tunnel interface (MTI)**—An MTI is the entrance or exit of an MT, equivalent to an entrance or exit of an MVPN. MTIs are automatically created when the MVPN for the VPN instance is created. PEs use the MTI to access the MT. The local PE sends VPN data out of the MTI. The remote PEs receive the private data from their MTIs. An MTI runs the same PIM mode as the VPN instance to which the MTI belongs. PIM is enabled on MTIs when a minimum of one interface in the VPN instance is enabled with PIM. When PIM is disabled on all interfaces in the VPN instance, PIM is also disabled on MTIs.
- **Default-group**—A default group is a unique multicast address assigned to each MVPN on the public network. It is the unique identifier of an MVPN on the public network and helps build the default MDT for an MVPN on the public network. A PE encapsulates a VPN multicast packet (a multicast protocol packet or a multicast data packet) into a public network multicast packet. The default group address is used as the public network multicast group.
- **Default MDT**—A default MDT uses a default group address as its group address. In a VPN, the default MDT is uniquely identified by the default group. A default MDT is automatically created after the default group is specified and will always exist on the public network, regardless of the presence of any multicast services on the public network or the VPN.
- **Data group**—An MVPN is assigned a unique data group for MDT switchover. The ingress PE selects a least used address from the data group range to encapsulate the VPN multicast packets when the multicast traffic of the VPN reaches or exceeds a threshold. Other PEs are notified to use the address to forward the multicast traffic for that VPN. This initiates the switchover to the data MDT.
- **Data MDT**—A data MDT is an MDT that uses a data group as it group address. At MDT switchover, PEs with downstream receivers join a data group to build a data MDT. The ingress PE forwards the encapsulated VPN multicast traffic along the data MDT over the public network.

How MDT-based MVPN works

For a VPN instance, multicast data transmission on the public network is transparent. The VPN data is exchanged between the MTIs of the local PE and the remote PE. This implements the seamless transmission of the VPN data over the public network. However, the multicast data transmission process (the MDT transmission process) over the public network is very complicated.

NOTE:

The following types of PIM neighboring relationships exist in MVPN:

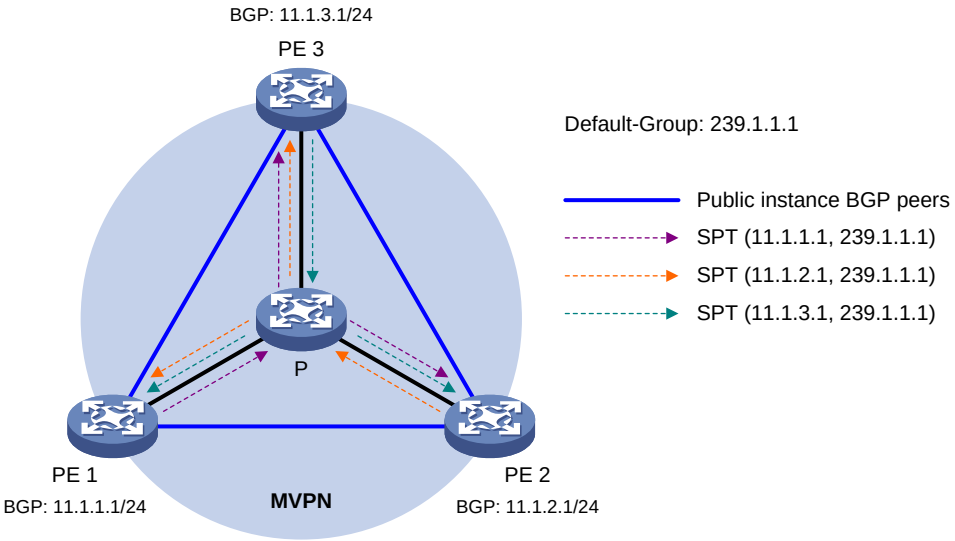
- **PE-P PIM neighboring relationship**—Established between the public network interface on a PE and the peer interface on the P device over the link.
- **PE-PE PIM neighboring relationship**—Established between PEs that are in the same VPN instance after they receive the PIM hello packets.
- **PE-CE PIM neighboring relationship**—Established between a PE interface that is bound with the VPN instance and the peer interface on the CE over the link.

Default MDT establishment

The multicast routing protocol running on the public network can be PIM-DM, PIM-SM, BIDIR-PIM, or PIM-SSM. The process of creating a Default MDT is different in these PIM modes.

Default MDT establishment in a PIM-DM network

Figure 2 Default MDT establishment in a PIM-DM network



As shown in Figure 2, PIM-DM is enabled on the network, and all the PEs support VPN instance A. The process of establishing a default MDT is as follows:

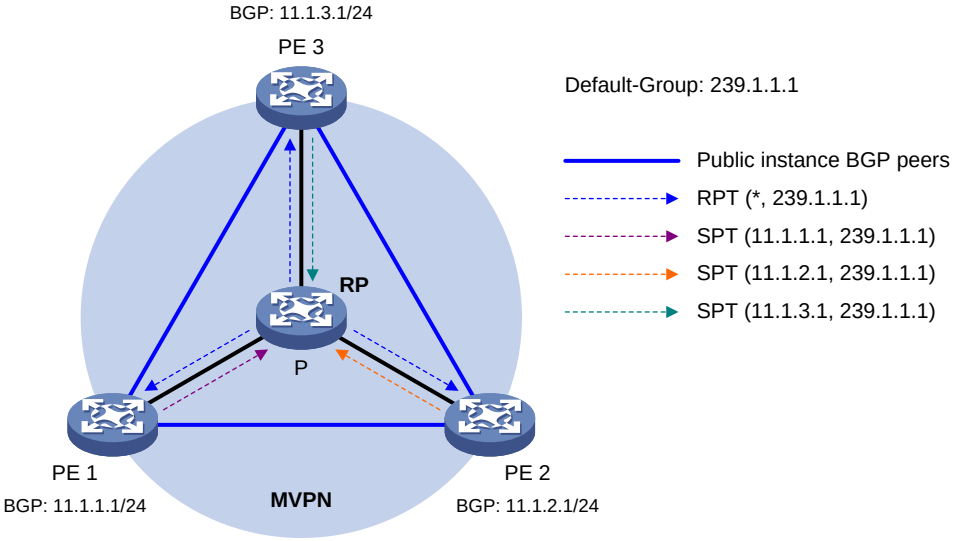
1. To establish PIM neighboring relationships with PE 2 and PE 3 through the MTI for VPN instance A, PE 1 does the following:
   a. Encapsulates the PIM protocol packet of the private network into a public network multicast data packet. PE 1 does this by specifying the source address as the IP address of the MVPN source interface and the multicast group address as the default group address.
   b. Sends the multicast data packet to the public network.

   For other PEs that support VPN instance A as default group members, PE 1 of VPN instance A initiates a flood-prune process in the entire public network. A (11.1.1.1, 239.1.1.1) state entry is created on each device along the path on the public network. This forms an SPT with PE 1 as the root, and PE 2 and PE 3 as leaves.
2. At the same time, PE 2 and PE 3 separately initiate a similar flood-prune process.

   Finally, three independent SPTs are established in the MVPN, constituting the default MDT in the PIM-DM network.

Default MDT establishment in a PIM-SM network

Figure 3 Default MDT establishment in a PIM-SM network



As shown in Figure 3, PIM-SM is enabled on the network, and all the PEs support VPN instance A. The process of establishing a default MDT is as follows:

1. PE 1 initiates a join to the public network RP by specifying the multicast group address as the default group address in the join message. A (*, 239.1.1.1) state entry is created on each device along the path on the public network.
2. At the same time, PE 2 and PE 3 separately initiate a similar join process.

   Finally, an RPT is established in the MVPN, with the public network RP as the root and PE 1, PE 2, and PE 3 as leaves.
3. To establish PIM neighboring relationships with PE 2 and PE 3 through the MTI for VPN instance A, PE 1 does the following:

   a. Encapsulates the PIM protocol packet of the private network into a public network multicast data packet. PE 1 does this by specifying the source address as the IP address of the MVPN source interface and the multicast group address as the default group address.

   b. Sends the multicast data packet to the public network.

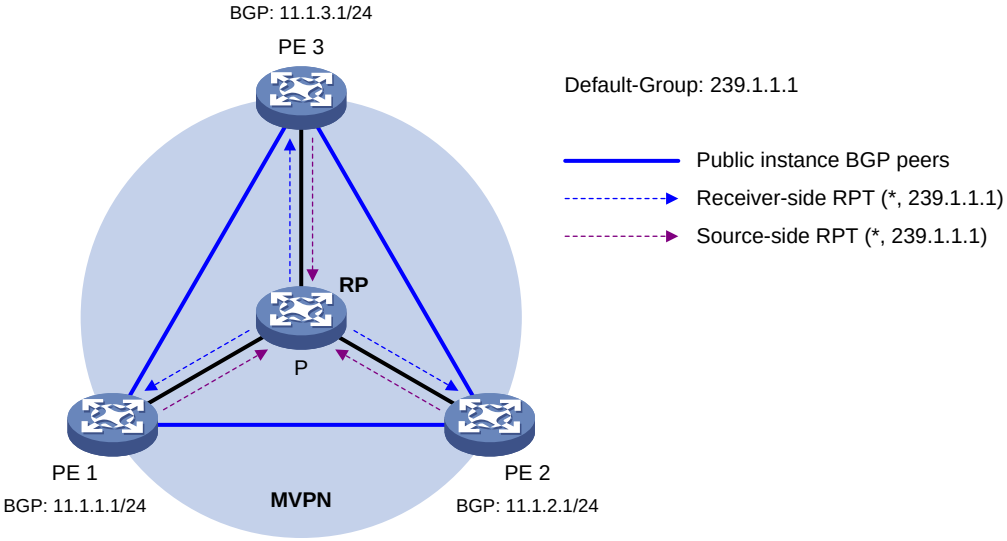
   The public network interface of PE 1 registers the multicast source with the public network RP, and the public network RP initiates a join to PE 1. A (11.1.1.1, 239.1.1.1) state entry is created on each device along the path on the public network.
4. At the same time, PE 2 and PE 3 separately initiate a similar register process.

   Finally, three SPTs between the PEs and the RP are established in the MVPN.

In the PIM-SM network, the RPT, or the (*, 239.1.1.1) tree, and the three independent SPTs constitute the default MDT.

Default MDT establishment in a BIDIR-PIM network

Figure 4 Default MDT establishment in a BIDIR-PIM network



As shown in Figure 4, BIDIR-PIM runs on the network, and all the PEs support VPN instance A. The process of establishing a default MDT is as follows:

1. PE 1 initiates a join to the public network RP by specifying the multicast group address as the default group address in the join message. A (*, 239.1.1.1) state entry is created on each device along the path on the public network.

   At the same time, PE 2 and PE 3 separately initiate a similar join process. Finally, a receiver-side RPT is established in the MVPN, with the public network RP as the root and PE 1, PE 2, and PE 3 as leaves.

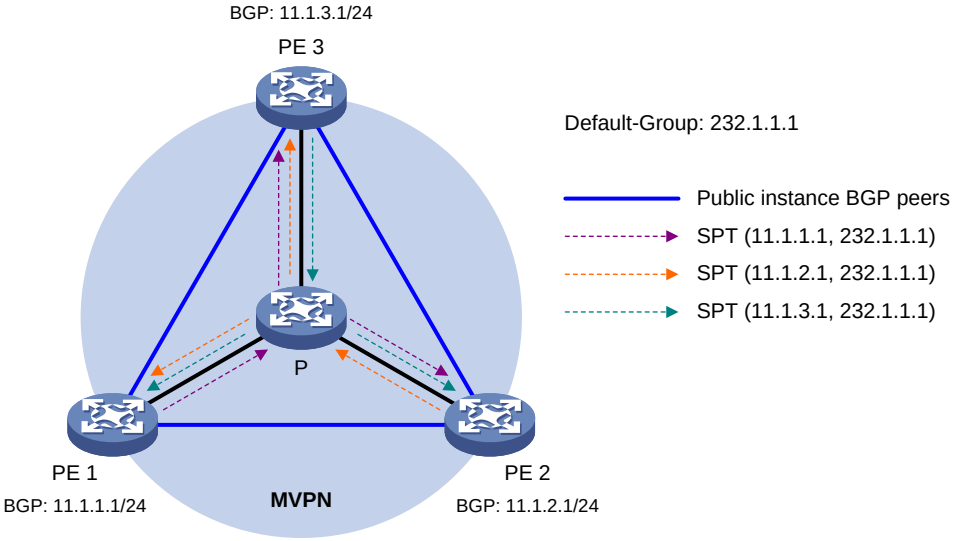
2. PE 1 sends a multicast packet with the default group address as the multicast group address. The DF of each network segment on the public network forwards the multicast packet to the RP. Each device on the path creates a (*, 239.1.1.1) state entry.

   At the same time, PE 2 and PE 3 separately initiate a similar process. Finally, three source-side RPTs are established in the MVPN, with PE 1, PE 2, and PE 3 as the roots and as the public network RP as the leave.

3. The receiver-side RPT and the three source-side RPTs constitute the default MDT in the BIDIR-PIM network.

Default MDT establishment in a PIM-SSM network

Figure 5 Default MDT establishment in a PIM-SSM network



As shown in Figure 5, PIM-SSM runs on the network, and all the PEs support VPN instance A. The process of establishing a default MDT is as follows:

1. PE 1, PE 2, and PE 3 exchange MDT route information (including BGP interface address and the default group address) through BGP.
2. PE 1 sends a subscribe message to PE 2 and PE 3. Each device on the public network creates an (S, G) entry. An SPT is established in the MVPN with PE 1 as the root and PE 2 and PE 3 as the leaves.

   At the same time, PE 2 and PE 3 separately initiate a similar process, and establish an SPT with itself as the root and the other PEs as the leaves.
3. The three independent SPTs constitute the default MDT in the PIM-SSM network.

In PIM-SSM, the term "subscribe message" refers to a join message.

Default MDT characteristics

No matter which PIM mode is running on the public network, the default MDT has the following characteristics:

- All PEs that support the same VPN instance join the default MDT.
- All multicast packets that belong to this VPN are forwarded along the default MDT to every PE on the public network, even if no active downstream receivers exist.

Default MDT-based delivery

After the default MDT is established, the multicast source forwards the VPN multicast data to the receivers in each site along the default MDT. The VPN multicast packets are encapsulated into public network multicast packets on the local PE, and transmitted along the default MDT. Then, they are decapsulated on the remote PE and transmitted in that VPN site.

VPN multicast data packets are forwarded across the public network differently in the following circumstances:

- If PIM-DM or PIM-SSM is running in the VPN, the multicast source forwards multicast data packets to the receivers along the VPN SPT across the public network.
- When PIM-SM is running in the VPN:
  - Before the RPT-to-SPT switchover, if the multicast source and the VPN RP are in different sites, the VPN multicast data packets travel to the VPN RP along the VPN SPT across the

public network. If the VPN RP and the receivers are in different sites, the VPN multicast data packets travel to the receivers along the VPN RPT over the public network.

- After the RPT-to-SPT switchover, if the multicast source and the receivers are in different sites, the VPN multicast data packets travel to the receivers along the VPN SPT across the public network.

- When BIDIR-PIM is running in the VPN, if the multicast source and the VPN RP are in different sites, the multicast source sends multicast data to the VPN RP across the public network along the source-side RPT. If the VPN RP and the receivers are in different sites, the multicast data packets travel to the receivers across the public network along the receiver-side RPT.

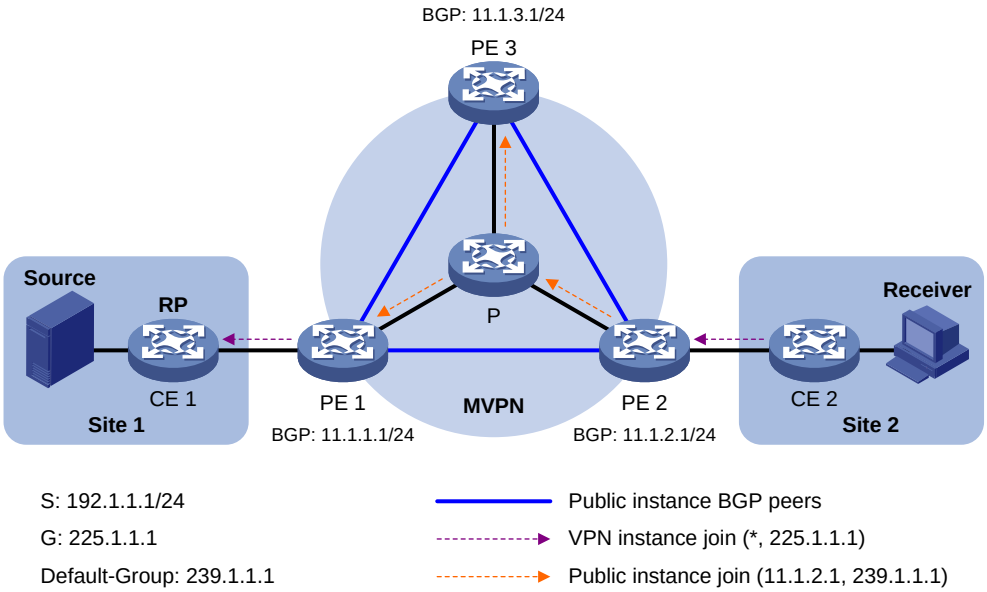
  For more information about RPT-to-SPT switchover, see "PIM overview."

The following example explains how multicast data packets are delivered based on the default MDT when PIM-DM is running in both the public network and the VPN network.

As shown in Figure 6:

- PIM-DM is running in both the public network and the VPN sites.
- Receiver of the VPN multicast group G (225.1.1.1) in Site 2 is attached to CE 2.
- Source in Site 1 sends multicast data to multicast group (G).
- The default group address used to forward public network multicast data is 239.1.1.1.

Figure 6 Multicast data packet delivery



A VPN multicast data packet is delivered across the public network as follows:

1. Source sends a VPN multicast data packet (192.1.1.1, 225.1.1.1) to CE 1.
2. CE 1 forwards the VPN multicast data packet along an SPT to PE 1, and the VPN instance on PE 1 examines the MVRF.

   If the outgoing interface list of the forwarding entry contains an MTI, PE 1 processes the VPN multicast data packet as described in step 3. The VPN instance on PE 1 considers the VPN multicast data packet to have been sent out of the MTI, because step 3 is transparent to it.
3. PE 1 encapsulates the VPN multicast data packet into a public network multicast packet (11.1.2.1, 239.1.1.1) by using the GRE method. The source IP address of the packet is the MVPN source interface 11.1.1.1, and the destination address is the default group address 239.1.1.1. PE 1 then forwards it to the public network.
4. The default MDT forwards the multicast data packet (11.1.2.1, 239.1.1.1) to the public network instance on all the PEs. After receiving this packet, every PE decapsulates it to get the original

VPN multicast data packet, and passes it to the corresponding VPN instance. If a PE has a downstream interface for an SPT, it forwards the VPN multicast packet down the SPT. Otherwise, it discards the packet.

5. The VPN instance on PE 2 looks up the MVRF and finally delivers the VPN multicast data to Receiver.

   By now, the process of transmitting a VPN multicast data packet across the public network is completed.

MDT switchover

Switching from default MDT to data MDT

When a multicast packet of a VPN is transmitted through the default MDT on the public network, the packet is forwarded to all PEs that support that VPN instance. This occurs whether or not any active receivers exist in the attached sites. When the rate of the multicast traffic of that VPN is high, multicast data might get flooded on the public network. This increases the bandwidth use and brings extra burden on the PEs.

To optimize multicast transmission of large VPN multicast traffic that enters the public network, the MDT-based MVPN solution introduces a dedicated data MDT. The data MDT is built between the PEs that connect VPN multicast receivers and multicast sources. When specific network criteria are met, a switchover from the default MDT to the data MDT occurs to forward VPN multicast traffic to receivers.

The device initiates a switchover of the default MDT to the data MDT as follows:

1. The source-side PE (PE 1, for example) periodically examines the forwarding rate of the VPN multicast traffic. The default MDT switches to the data MDT only when the following criteria are both met:
   - The VPN multicast data has passed the ACL rule filtering for default MDT to data MDT switchover.
   - The traffic rate of the VPN multicast stream has exceeded the switchover threshold and stayed higher than the threshold for a certain length of time.
2. PE 1 selects a least-used address from the data group range. Then, it sends an MDT switchover message to all the other PEs down the default MDT. This message contains the VPN multicast source address, the VPN multicast group address, and the data group address.
3. Each PE that receives this message examines whether it interfaces with a VPN that has receivers of that VPN multicast stream.

   If so, it joins the data MDT rooted at PE 1. Otherwise, it caches the message and will join the data MDT when it has attached receivers.
4. After sending the MDT switchover message, PE 1 starts the data-delay timer. When the timer expires, PE 1 uses the default group address to encapsulate the VPN multicast data. The multicast data is then forwarded down the data MDT.
5. After the multicast traffic is switched from the default MDT to the data MDT, PE 1 continues sending MDT switchover messages periodically. Subsequent PEs with attached receivers can then join the data MDT. When a downstream PE no longer has active receivers attached to it, it leaves the data MDT.

For a given VPN instance, the default MDT and the data MDT are both forwarding tunnels in the same MVPN. A default MDT is uniquely identified by a default group address, and a data MDT is uniquely identified by a data group address. Each default group is uniquely associated with a data group range.

Backward switching from data MDT to default MDT

After the VPN multicast traffic is switched to the data MDT, the multicast traffic conditions might change and no longer meet the switchover criterion. In this case, PE 1, as in the preceding example, initiates a backward MDT switchover process when any of the following criteria are met:

- The traffic rate of the VPN multicast data has dropped below the switchover threshold. In addition, the traffic rate has stayed lower than the threshold for a certain length of time (known as the data holddown period).
- The associated data group range is changed, and the data group address for encapsulating the VPN multicast data is out of the new address range.
- The ACL rule for controlling the switchover from the default MDT to the data MDT has changed, and the VPN multicast data fails to pass the new ACL rule.

Inter-AS MDT-based MVPN

In an inter-AS VPN networking scenario, VPN sites are located in multiple ASs. These sites must be interconnected. Inter-AS VPN provides the following solutions:

- **VRF-to-VRF connections between ASBRs**—This solution is also called inter-AS option A.
- **EBGP redistribution of labeled VPN-IPv4 routes between ASBRs**—ASBRs advertise VPN-IPv4 routes to each other through MP-EBGP. This solution is also called inter-AS option B.
- **Multihop EBGP redistribution of labeled VPN-IPv4 routes between PE devices**—PEs advertise VPN-IPv4 routes to each other through MP-EBGP. This solution is also called inter-AS option C.

For more information about the three inter-AS VPN solutions, see MPLS L3VPN configuration in *MPLS Configuration Guide*.

Based on these solutions, there are three ways to implement inter-AS MVPN:

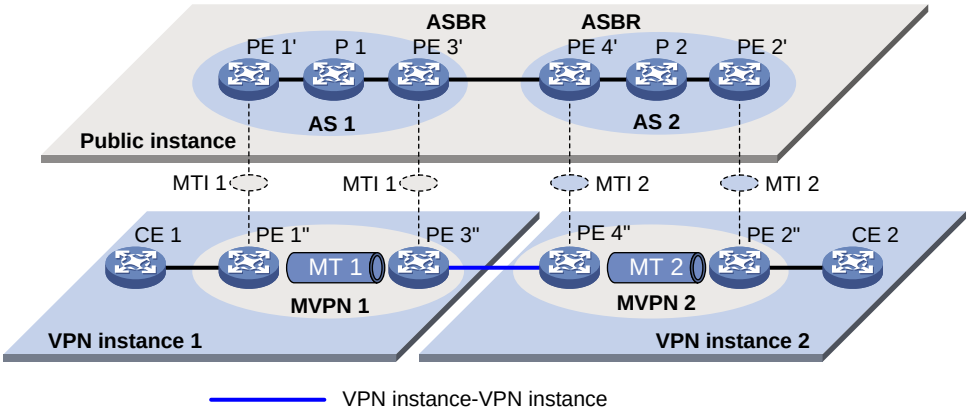
- MDT-based MVPN inter-AS option A.
- MDT-based MVPN inter-AS option B.
- MDT-based MVPN inter-AS option C.

MDT-based MVPN inter-AS option A

As shown in Figure 7:

- Two VPN instances are in AS 1 and AS 2.
- PE 3 and PE 4 are ASBRs for AS 1 and AS 2, respectively.
- PE 3 and PE 4 are interconnected through their respective VPN instance and treat each other as a CE.

Figure 7 MVPN inter-AS option A



To implement MVPN inter-AS option A, a separate MVPN must be created in each AS. Multicast data is transmitted between the VPNs in different ASs through the MDs.

Multicast packets of VPN instance 1 are delivered as follows:

1. CE 1 forwards the multicast packet of VPN instance 1 to PE 1.

2. PE 1 encapsulates the multicast packet into a public network packet and forwards it to PE 3 through the MTI interface in MVPN 1.
3. PE 3 considers PE 4 as a CE of VPN instance 1, so PE 3 forwards the multicast packet to PE 4.
4. PE 4 considers PE 3 as a CE of VPN instance 2, so it forwards the multicast packet to PE 2 through the MTI interface in MVPN 2 on the public network.
5. PE 2 forwards the multicast packet to CE 2.

Because only VPN multicast data is forwarded between ASBRs, different PIM modes can run within different ASs. However, the same PIM mode must run on all interfaces that belong to the same VPN (including interfaces with VPN bindings on ASBRs).

MDT-based MVPN inter-AS option B

In MVPN inter-AS option B, RPF vector and BGP connector are introduced:

- **RPF vector**—Attribute encapsulated in a PIM join message. It is the next hop of BGP MDT route from the local PE to the remote PE. Typically, it is the ASBR in the local AS.

  When a device receives the join message with the RPF vector, it first checks whether the RPF vector is its own IP address. If so, the device removes the RPF vector, and sends the message to its upstream neighbor according to the route to the remote PE. Otherwise, it keeps the RPF vector, looks up the route to the RPF vector, and sends the message to the next hop of the route. In this way, the PIM message can be forwarded across the ASs and an MDT is established.
- **BGP connector**—Attribute shared by BGP peers when they exchange IPv4 VPN routes. It is the IP address of the remote PE.

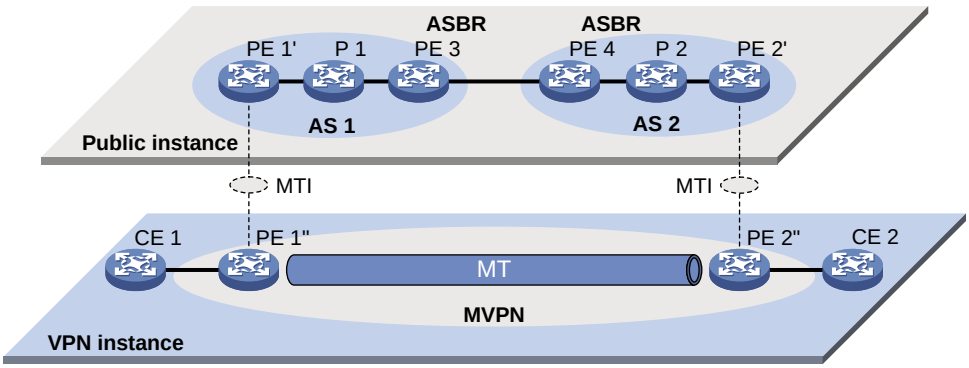
  The local PE fills the upstream neighbor address field with the BGP connector in a join message. This ensures that the message can pass the RPF check on the remote PE after it travels along the MT.

To implement MVPN inter-AS option B, only one MVPN needs to be established for the two ASs. VPN multicast data is transmitted between different ASs on the public network within this MVPN.

As shown in Figure 8:

- A VPN network involves AS 1 and AS 2.
- PE 3 and PE 4 are the ASBRs for AS 1 and AS 2, respectively.
- PE 3 and PE 4 are interconnected through MP-EBGP and treat each other as a P device.
- PE 3 and PE 4 advertise VPN-IPv4 routes to each other through MP-EBGP.
- An MT is established between PE 1 and PE 2 for delivering VPN multicast traffic across the ASs.

Figure 8 MVPN inter-AS option B



The establishment of the MDT on the public network is as follows:

1. PE 1 originates a PIM join message to join the SPT rooted at PE 2. In the join message, the upstream neighbor address is the IP address of PE 2 (the BGP connector). The RPF vector

attribute is the IP address of PE 3. PE 1 encapsulates the join message as a public network packet and forwards it through the MTI.

2. P 1 determines that the RPF vector is not an IP address of its own. It looks up the routing table for a route to PE 3, and forwards the packet to PE 3.
3. PE 3 removes the RPF vector because the RPF vector is its own IP address. It fails to find a BGP MDT route to PE 2, so it encapsulates a new RPF vector (IP address of PE 4) in the packet and forwards it to PE 4.
4. PE 4 removes the RPF vector because the RPF vector is its own IP address. It has a local route to PE 2, so it forwards the packet to P 2, which is the next hop of the route to PE 2.
5. P 2 sends the packet to PE 2.
6. PE 2 receives the packet on the MTI and decapsulates the packet. The receiving interface is the RPF interface of the RPF route back to PE 1 for the join message, and the join message passes the RPF check. The SPT from PE 1 to PE 2 is established.

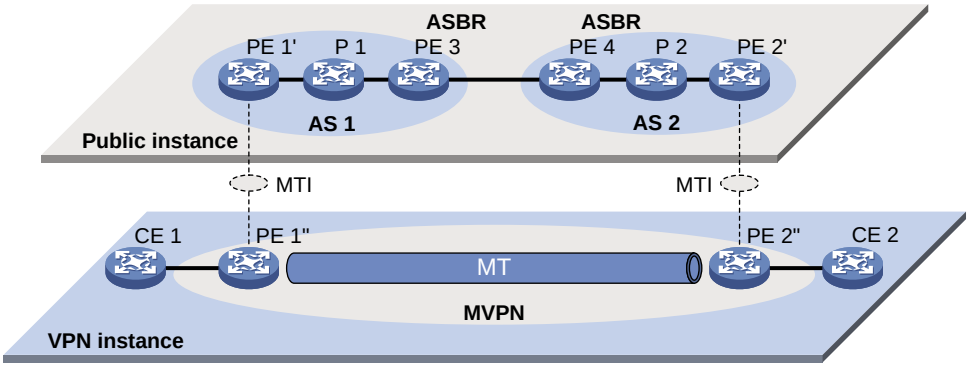
When PE 1 joins the SPT rooted at PE 1, PE 2 also initiates a join process to the SPT rooted at PE 1. A MDT is established when the two SPTs are finished.

MDT-based MVPN inter-AS option C

As shown in Figure 9:

- A VPN network involves AS 1 and AS 2.
- PE 3 and PE 4 are the ASBRs for AS 1 and AS 2, respectively.
- PE 3 and PE 4 are interconnected through MP-EBGP and treat each other as a P device.
- PEs in different ASs establish a multihop MP-EBGP session to advertise VPN-IPv4 routes to each other.

Figure 9 MVPN inter-AS option C



To implement MVPN inter-AS option C, only one MVPN needs to be created for the two ASs. Multicast data is transmitted between the two ASs through the MVPN.

Multicast packets are delivered as follows:

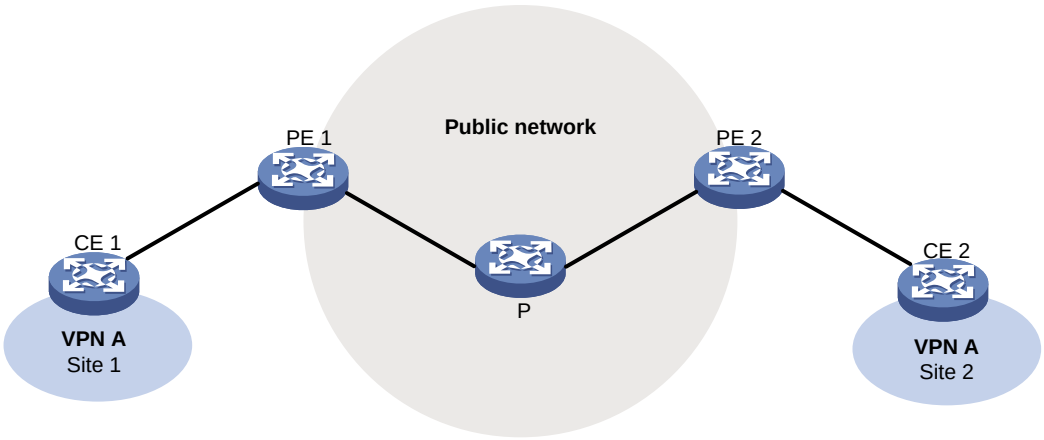
1. CE 1 forwards the VPN instance multicast packet to PE 1.
2. PE 1 encapsulates the multicast packet into a public network multicast packet and forwards it to PE 3 through the MTI interface on the public network.
3. PE 3 and PE 4 are interconnected through MP-EBGP, so PE 3 forwards the public network multicast packet to PE 4 along the VPN IPv4 route.
4. The public network multicast packet arrives at the MTI interface of PE 2 in AS 2. PE 2 decapsulates the public network multicast packet and forwards the VPN multicast packet to CE 2.

M6VPE

The multicast IPv6 VPN provider edge (M6VPE) feature enables PEs to transmit IPv6 multicast traffic of a VPN instance over the public network. Only the IPv4 network is available for the backbone network.

As shown in Figure 10, the public network runs IPv4 protocols, and sites of VPN instance **VPN A** run IPv6 multicast protocols. To transmit IPv6 multicast traffic between CE 1 and CE 2, configure M6VPE on the PEs.

Figure 10 M6VPE network



IPv6 multicast traffic forwarding over the IPv4 public network is as follows:

1. CE 1 forwards an IPv6 multicast packet for VPN instance **VPN A** to PE 1.
2. PE 1 encapsulates the IPv6 multicast packet with an IPv4 packet header and transmits the IPv4 packet in the IPv4 backbone network.
3. PE 2 decapsulates the IPv4 packet and forwards the IPv6 multicast packet to CE 2.

Protocols and standards

- RFC 6037, *Cisco Systems' Solution for Multicast in BGP/MPLS IP VPNs*
- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*

MDT-based MVPN tasks at a glance

To configure MDT-based MVPN, perform the following tasks on PEs:

1. Configuring MDT-based MVPN
   a. Enabling IP multicast routing for a VPN instance
   b. Creating an MDT-based MVPN instance
   c. Creating an MVPN address family
   d. Specifying the default group
   e. Specifying the MVPN source interface
   f. (Optional.) Configuring MDT switchover parameters
   g. (Optional.) Configuring the RPF vector feature
   h. (Optional.) Enabling data group reuse logging
   i. (Optional.) Setting the DSCP value for outgoing data group switchover packets

2. Configuring BGP MDT

   If PIM-SSM is running on the public network, you must configure BGP MDT.

   a. Configuring BGP MDT peers or peer groups

   b. (Optional.) Configuring a BGP MDT route reflector

   c. (Optional.) Configuring BGP MDT optimal route selection delay

Configuring MDT-based MVPN

Prerequisites for configuring MDT-based MVPN

Before you configure MDT-based MVPN, complete the following tasks:

- Configure a unicast routing protocol on the public network.
- Configure MPLS L3VPN on the public network.
- Configure PIM-DM, PIM-SM, BIDIR-PIM, or PIM-SSM on the public network.

Enabling IP multicast routing for a VPN instance

To enable IP multicast routing for a VPN instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VPN instance and enter its view.	**ip vpn-instance** *vpn-instance-name*	For more information about this command, see *MPLS Command Reference*.
3. Configure an RD for the VPN instance.	**route-distinguisher** *route-distinguisher*	For more information about this command, see *MPLS Command Reference*.
4. Return to system view.	**quit**	N/A
5. Enter interface view.	**interface** *interface-type interface-number*	N/A
6. Associate the interface with the VPN instance.	**ip binding vpn-instance** *vpn-instance-name*	By default, an interface is associated with no VPN instance and belongs to the public network. For more information about this command, see *MPLS Command Reference*.
7. Return to system view.	**quit**	N/A
8. Enable IP multicast routing for the VPN instance and enter MRIB view of the VPN instance.	IPv4: **multicast routing vpn-instance** *vpn-instance-name* IPv6: **ipv6 multicast routing vpn-instance** *vpn-instance-name*	*By default, IPv4 multicast routing is disabled for a VPN instance.* *For more information about this command, see IP Multicast Command Reference.* *By default, IPv6 multicast routing is disabled for a VPN instance.* *For more information about this command, see IP Multicast Command Reference.*

Creating an MDT-based MVPN instance

About creating an MDT-based MVPN instance

To provide multicast services for a VPN instance, you must create an MDT-based MVPN instance on PEs that belong to the VPN instance. After the MVPN instance is created, the system automatically creates MTIs and binds them with the VPN instance.

You can create one or more MDT-based MVPN instances on a PE.

Procedure

To create an MDT-based MVPN instance:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an MDT-based MVPN instance and enter MVPN view.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A

Creating an MVPN address family

About creating an MVPN address family

You must create an MVPN IPv4 or IPv6 address family for a VPN instance before you can perform other MVPN VPN configuration tasks for the VPN instance. For a VPN instance, configurations in MVPN IPv4 and IPv6 address family views apply to IPv4 and IPv6 multicast packets of the instance, respectively.

Procedure

To create an MVPN address family:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MVPN view of a VPN instance.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A
3. Create an MVPN address family and enter MVPN address family view.	IPv4: **address-family ipv4** IPv6: **address-family ipv6**	

Specifying the default group

Restrictions and guidelines

You must specify the same default group on all PEs that belong to the same MVPN.

The default group for an MVPN must be different from the default group and the data group used by any other MVPN.

For an MVPN that transmits both IPv4 and IPv6 multicast packets, you must specify the same default group in MVPN IPv4 address family view and IPv6 address family view.

Procedure

To specify the default group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MVPN view.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A
3. Enter MVPN address family view.	IPv4: **address-family ipv4** IPv6: **address-family ipv6**	
4. Specify the default group.	**default-group** *group-address*	N/A

Specifying the MVPN source interface

About MVPN source interfaces

An MTI of a VPN instance uses the IP address of the MVPN source interface as the source address to encapsulate multicast packets for the VPN instance.

Restrictions and guidelines

For the PE to obtain correct routing information, you must specify the interface used for establishing BGP peer relationship as the MVPN source interface.

For an MVPN that transmits both IPv4 and IPv6 multicast packets, you must specify the same MVPN source interface in MVPN IPv4 and IPv6 address family views.

The MTI takes effect only after the default group and MVPN source interface are specified and the MTI obtains the public IP address of the MVPN source interface. On some devices, for the MTI to forward packets, you must create a service loopback group of the multicast type. For more information about creating service loopback groups, see *Layer 2—LAN Switching Configuration Guide*.

Procedure

To specify the MVPN source interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MVPN view.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A
3. Enter MVPN address family view.	IPv4: **address-family ipv4** IPv6: **address-family ipv6**	
4. Specify the MVPN source interface.	**source** *interface-type interface-number*	By default, no MVPN source interface is specified.

Configuring MDT switchover parameters

About MDT switchover parameters

To decrease traffic interruption caused by frequent default-MDT to data-MDT switchovers, you can adjust the data-delay period. The switchover occurs a data-delay period after the multicast VPN data first arrives, regardless of whether multicast VPN data keeps arriving during the period.

Restrictions and guidelines

On a PE, the data group range for an MVPN cannot include the default group or data groups of any other MVPN.

All VPN instances share the data group resources. As a best practice to avoid data group resource exhaustion, specify a reasonable data group range for a VPN instance.

For an MVPN that transmits both IPv4 and IPv6 multicast packets, the data group range in MVPN IPv4 and IPv6 address family views cannot overlap.

If the public network runs PIM-SSM, the data group range for an MVPN on a PE can overlap with data group ranges for other MDs on other PEs.

Procedure

To configure MDT switchover parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MVPN view.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A
3. Enter MVPN address family view.	IPv4: **address-family ipv4** IPv6: **address-family ipv6**	
4. Configure the data group range and the switchover criteria.	**data-group** *group-address* { *mask-length* | *mask* } [**acl** *acl-number*]	By default, no data group range exists, and the default MDT to data MDT switchover never occurs.
5. Set the data-delay period.	**data-delay** *delay*	By default, the data-delay period is 3 seconds.
6. Set the data holddown period.	**data-holddown** *delay*	By default, the data holddown period is 60 seconds.

Configuring the RPF vector feature

About the RPF vector feature

This feature enables the device to insert the RPF vector (IP address of the ASBR in the local AS) in PIM join messages for other devices to perform RPF check.

Restrictions and guidelines

Perform this task on PEs that have attached receivers.

For the device to work with other manufacturers' products on the RPF vector, you must enable RPF vector compatibility for all HPE P devices and HPE PE devices on the public network.

Procedure

To enable RPF vector compatibility:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MRIB view of a VPN instance.	**multicast routing vpn-instance** *vpn-instance-name*	N/A
3. Enable the RPF vector feature.	**rpf proxy vector**	By default, the RPF vector feature is disabled.
4. Enable RPF vector compatibility.	**multicast rpf-proxy-vector compatible**	By default, RPF vector compatibility is disabled.

Enabling data group reuse logging

About data group reuse logging

For a given VPN, the number of VPN multicast streams to be switched to data MDTs might exceed the number of addresses in the data group range. In this case, the VPN instance on the source-side PE can reuse the addresses in the address range. With data group reuse logging enabled, the address reuse information will be logged. Perform this task on PEs.

The group address reuse logging information has a severity level **informational**. For more information about the logging information, see *Network Management and Monitoring Configuration Guide*.

Procedure

To enable data group reuse logging:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MVPN view.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A
3. Enter MVPN address family view.	IPv4: **address-family ipv4** IPv6: **address-family ipv6**	
4. Enable data group reuse logging.	**log data-group-reuse**	By default, data group reuse logging is disabled.

Setting the DSCP value for outgoing data group switchover packets

About the DSCP value for outgoing data group switchover packets

The DSCP value determines the packet transmission priority. A greater DSCP value represents a higher priority.

Procedure

To set the DSCP value for outgoing data group switchover packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter MVPN view.	**multicast-vpn vpn-instance** *vpn-instance-name* **mode mdt**	N/A
3. Setting the DSCP value for outgoing data group switchover packets.	**dscp** *dscp-value*	By default, the DSCP value is 48 for outgoing data group switchover packets.

Configuring BGP MDT

Configuring BGP MDT peers or peer groups

About BGP MDT peers and peer groups

Perform this task so that the PE can exchange MDT information with the BGP peer or peer group. MDT information includes the IP address of the PE and default group to which the PE belongs. On a public network running PIM-SSM, the multicast VPN establishes a default MDT rooted at the PE (multicast source) based on the MDT information.

Prerequisites

Before you configure a BGP MDT peer or peer group, you must create a BGP peer or peer group in BGP instance view. For more information about creating a BGP peer or peer group, see BGP configuration in *Layer 3—IP Routing Configuration Guide*.

Procedure

To configure BGP MDT peers or peer groups:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP instance view.	**bgp** *as-number* [**instance** *instance-name*]	N/A
3. Create a BGP IPv4 MDT address family and enter its view.	**address-family ipv4 mdt**	By default, no BGP IPv4 address family exists.
4. Enable the device to exchange MDT routing information with the BGP peer or the peer group.	**peer** { *group-name* | *ip-address* [*mask-length*] } **enable**	By default, the device cannot exchange BGP MDT routing information with a BGP peer or peer group. For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.

Configuring a BGP MDT route reflector

About configuring BGP MDT route reflectors

- **Configuring a BGP MDT route reflector**—BGP MDT peers in the same AS must be fully meshed to maintain connectivity. However, when multiple BGP MDT peers exist in an AS, connection establishment among them might result in increased costs. To reduce connections between BGP MDT peers, you can configure one of them as a route reflector and specify other devices as clients.

- **Disabling routing reflection between clients**—When clients establish BGP MDT connections with the route reflector, the route reflector forwards (or reflects) BGP MDT routing information between clients. The clients are not required to be fully meshed. To save bandwidth if the clients have been fully meshed, you can disable the routing reflection between clients by using the **undo reflect between-clients** command.
- **Configuring the cluster ID of the route reflector**—The route reflector and its clients form a cluster. Typically, a cluster has only one route reflector whose router ID identifies the cluster. However, you can configure several route reflectors in a cluster to improve network reliability. To avoid routing loops, make sure the route reflectors in a cluster have the same cluster ID.

Procedure

To configure BGP MDT route reflectors:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP instance view.	**bgp** *as-number* [**instance** *instance-name*]	N/A
3. Enter BGP IPv4 MDT address family view.	**address-family ipv4 mdt**	N/A
4. Configure the device as a route reflector and specify its peers or peer groups as clients.	**peer** { *group-name* | *ip-address* [*mask-length*] } **reflect-client**	By default, neither route reflectors nor clients exist.
5. (Optional.) Disable route reflection between clients.	**undo reflect between-clients**	By default, route reflection between clients is disabled. For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.
6. (Optional.) Configure the cluster ID of the route reflector.	**reflector cluster-id** { *cluster-id* | *ip-address* }	By default, a route reflector uses its router ID as the cluster ID. For more information about this command, see BGP commands in *Layer 3—IP Routing Command Reference*.

Configuring BGP MDT optimal route selection delay

To set the optimal route selection delay timer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter BGP instance view.	**bgp** *as-number* [**instance** *instance-name*]	N/A
3. Enter BGP IPv4 MDT address family view.	**address-family ipv4 mdt**	N/A
4. Set the optimal route selection delay timer.	**route-select delay** *delay-value*	By default, the optimal route selection delay timer is 0 seconds, which means optimal route selection is not delayed. For more information about this command, see BGP commands in *Layer 3—IP Routing Command*

Step	Command	Remarks
		Reference.

Display and maintenance commands for multicast VPN

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

Display and maintenance commands for MDT-based MVPN:

Task	Command
Display BGP MDT peer group information.	**display bgp** [**instance** *instance-name*] **group ipv4 mdt** [**group-name** *group-name*]
Display information about BGP MDT peers or peer groups.	**display bgp** [**instance** *instance-name*] **peer ipv4 mdt** [*ip-address mask-length* | { *ip-address* | **group-name** *group-name* } **log-info** | [*ip-address*] **verbose**]
Display information about BGP MVPN peers or peer groups.	**display bgp** [**instance** *instance-name*] **peer ipv4 mvpn** [*ip-address mask-length* | { *ip-address* | **group-name** *group-name* } **log-info** | [*ip-address*] **verbose**]
Display BGP MDT routing information.	**display bgp** [**instance** *instance-name*] **routing-table ipv4 mdt** [**route-distinguisher** *route-distinguisher*] [*ip-address* [**advertise-info**]]
Display information about BGP update groups for the BGP IPv4 MDT address family.	**display bgp** [**instance** *instance-name*] **update-group ipv4 mdt** [*ip-address*]
Display information about data groups for IPv4 multicast transmission that are received in a VPN instance.	**display multicast-vpn vpn-instance** *vpn-instance-name* **data-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *]
Display information about data groups for IPv6 multicast transmission that are received in a VPN instance.	**display multicast-vpn vpn-instance** *vpn-instance-name* **ipv6 data-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [*mask-length*] | *vpn-group-address* [*mask-length*]] *]
Display information about data groups for IPv4 multicast transmission that are sent in a VPN instance.	**display multicast-vpn vpn-instance** *vpn-instance-name* **data-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *
Display information about data groups for IPv6 multicast transmission that are sent in a VPN instance.	**display multicast-vpn vpn-instance** *vpn-instance-name* **ipv6 data-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [*mask-length*] | *vpn-group-address* [*mask-length*]] *
Display information about default groups for IPv4 multicast transmission.	**display multicast-vpn** [**vpn-instance** *vpn-instance-name*] **default-group** { **local** | **remote** }
Display information about default groups for IPv6 multicast transmission.	**display multicast-vpn** [**vpn-instance** *vpn-instance-name*] **ipv6 default-group** { **local** | **remote** }
Reset BGP sessions for BGP IPv4 MDT address family.	**reset bgp** [**instance** *instance-name*] { *as-number* | *ip-address* [*mask-length*] | **all** | **external** | **group** *group-name* | **internal** } **ipv4 mdt**

For more information about the **display bgp group**, **display bgp peer**, **display bgp update-group**, and **reset bgp** commands, see BGP commands in *Layer 3—IP Routing Command Reference*.

Multicast VPN configuration examples

Example: Configuring intra-AS MDT-based MVPN

Network configuration

As shown in Figure 11, configure intra-AS MDT-based MVPN to meet the following requirements:

Item	Network configuration
Multicast sources and receivers	• In VPN instance **a**, S 1 is a multicast source, and R 1, R 2 and R 3 are receivers. • In VPN instance **b**, S 2 is a multicast source, and R 4 is a receiver. • For VPN instance **a**, the default group is 239.1.1.1, and the data group range is 225.2.2.0 to 225.2.2.15. • For VPN instance **b**, the default group is 239.2.2, and the data group range is 225.4.4.0 to 225.4.4.15.
VPN instances to which PE interfaces belong	• PE 1: VLAN-interface 11 and VLAN-interface 20 belong to VPN instance **a**. VLAN-interface 12 and Loopback 1 belong to the public network instance. • PE 2: VLAN-interface 13 belongs to VPN instance **b**. VLAN-interface 14 belongs to VPN instance **a**. VLAN-interface 15 and Loopback 1 belong to the public network instance. • PE 3: VLAN-interface 17 belongs to VPN instance **a**. VLAN-interface 18 and Loopback 2 belong to VPN instance **b**. VLAN-interface 19 and Loopback 1 belong to the public network instance.
Unicast routing protocols and MPLS	• Configure OSPF on the public network, and configure RIP between the PEs and CEs. • Establish BGP peer connections between PE 1, PE 2, and PE 3 on their respective Loopback 1. • Configure MPLS on the public network.
IP multicast routing	• Enable IP multicast routing on the P device. • Enable IP multicast routing on the public network on PE 1, PE 2, and PE 3. • Enable IP multicast routing for VPN instance **a** on PE 1, PE 2, and PE 3. • Enable IP multicast routing for VPN instance **b** on PE 2 and PE 3. • Enable IP multicast routing on CE a1, CE a2, CE a3, CE b1, and CE b2.
IGMP	• Enable IGMPv2 on VLAN-interface 20 of PE 1. • Enable IGMPv2 on VLAN-interface 40 of CE a2, VLAN-interface 50 of CE a3, and VLAN-interface 60 of CE b2.
PIM	Enable PIM-SM on the public network and for VPN instances **a** and **b**: • Enable PIM-SM on all interfaces of the P device. • Enable PIM-SM on all public and private network interfaces of PE 1, PE 2, and PE 3. • Enable PIM-SM on all interfaces that have no receiver hosts connected of CE a1, CE a2, CE a3, CE b1, and CE b2. • Configure Loopback 1 of P as a C-BSR and a C-RP for the public network to provide services for all multicast groups. • Configure Loopback 1 of CE a2 as a C-BSR and a C-RP for VPN instance **a** to provide services for all multicast groups. • Configure Loopback 2 of PE 3 as a C-BSR and a C-RP for VPN instance **b** to provide services for all multicast groups.

Figure 11 Network diagram

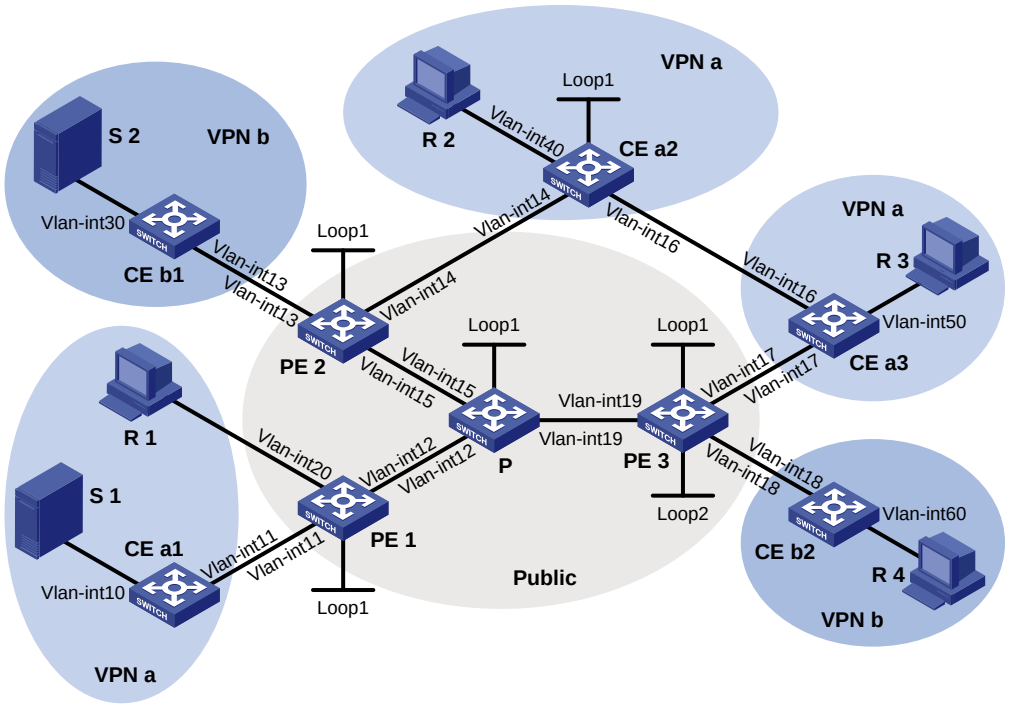


Table 3 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.110.7.2/24	PE 3	Vlan-int19	192.168.8.1/24
S 2	—	10.110.8.2/24	PE 3	Vlan-int17	10.110.5.1/24
R 1	—	10.110.1.2/24	PE 3	Vlan-int18	10.110.6.1/24
R 2	—	10.110.9.2/24	PE 3	Loop1	1.1.1.3/32
R 3	—	10.110.10.2/24	PE 3	Loop2	33.33.33.33/32
R 4	—	10.110.11.2/24	CE a1	Vlan-int10	10.110.7.1/24
P	Vlan-int12	192.168.6.2/24	CE a1	Vlan-int11	10.110.2.2/24
P	Vlan-int15	192.168.7.2/24	CE a2	Vlan-int40	10.110.9.1/24
P	Vlan-int19	192.168.8.2/24	CE a2	Vlan-int14	10.110.4.2/24
P	Loop1	2.2.2.2/32	CE a2	Vlan-int16	10.110.12.1/24
PE 1	Vlan-int12	192.168.6.1/24	CE a2	Loop1	22.22.22.22/32
PE 1	Vlan-int20	10.110.1.1/24	CE a3	Vlan-int50	10.110.10.1/24
PE 1	Vlan-int11	10.110.2.1/24	CE a3	Vlan-int17	10.110.5.2/24
PE 1	Loop1	1.1.1.1/32	CE a3	Vlan-int16	10.110.12.2/24
PE 2	Vlan-int15	192.168.7.1/24	CE b1	Vlan-int30	10.110.8.1/24
PE 2	Vlan-int13	10.110.3.1/24	CE b1	Vlan-int13	10.110.3.2/24
PE 2	Vlan-int14	10.110.4.1/24	CE b2	Vlan-int60	10.110.11.1/24
PE 2	Loop1	1.1.1.2/32	CE b2	Vlan-int18	10.110.6.2/24

Procedure

1. Configure PE 1:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
[PE1-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 11, VLAN 12, or VLAN 20.

```
[PE1] interface gigabitethernet 1/0/4
[PE1-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
```

Create a VPN instance named **a** and configure an RD and route targets for the VPN instance.

```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE1] multicast routing vpn-instance a
[PE1-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE1] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 family address for VPN instance **a**.

```
[PE1-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE1-mvpn-a-ipv4] default-group 239.1.1.1
[PE1-mvpn-a-ipv4] source loopback 1
[PE1-mvpn-a-ipv4] data-group 225.2.2.0 28
[PE1-mvpn-a-ipv4] quit
[PE1-mvpn-a] quit
```

Assign an IP address to VLAN-interface 12.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip address 192.168.6.1 24
```

#Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 12.

```
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] mpls enable
[PE1-Vlan-interface12] mpls ldp enable
[PE1-Vlan-interface12] quit
```

Associate VLAN-interface 20 with VPN instance **a**.

```
[PE1] interface vlan-interface 20
[PE1-Vlan-interface20] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 20, and enable IGMP on the interface.

```
[PE1-Vlan-interface20] ip address 10.110.1.1 24
[PE1-Vlan-interface20] igmp enable
[PE1-Vlan-interface20] quit
```

Associate VLAN-interface 11 with VPN instance **a**.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 11, and enable PIM-SM on the interface.

```
[PE1-Vlan-interface11] ip address 10.110.2.1 24
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

Configure BGP.

```
[PE1] bgp 100
[PE1-bgp-default] group vpn-g internal
[PE1-bgp-default] peer vpn-g connect-interface loopback 1
[PE1-bgp-default] peer 1.1.1.2 group vpn-g
[PE1-bgp-default] peer 1.1.1.3 group vpn-g
[PE1–bgp-default] ip vpn-instance a
[PE1-bgp-default-a] address-family ipv4
[PE1-bgp-default-ipv4-a] import-route rip 2
[PE1-bgp-default-ipv4-a] import-route direct
[PE1-bgp-default-ipv4-a] quit
[PE1-bgp-default-a] quit
[PE1–bgp-default] address-family vpnv4
[PE1–bgp-default-vpnv4] peer vpn-g enable
[PE1–bgp-default-vpnv4] quit
[PE1–bgp-default] quit
```

Configure OSPF.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 192.168.6.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure RIP.

```
[PE1] rip 2 vpn-instance a
[PE1-rip-2] network 10.110.1.0 0.0.0.255
[PE1-rip-2] network 10.110.2.0 0.0.0.255
[PE1-rip-2] import-route bgp
[PE1-rip-2] return
```

2. Configure PE 2:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE2> system-view
[PE2] router id 1.1.1.2
```

```
[PE2] multicast routing
[PE2-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE2] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 13, VLAN 14, or VLAN 15.

```
[PE2] interface gigabitethernet 1/0/4
[PE2-GigabitEthernet1/0/4] port service-loopback group 1
[PE2-GigabitEthernet1/0/4] quit
```

Configure an MPLS LSR ID, and enable LDP globally.

```
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls ldp
[PE2-ldp] quit
```

Create a VPN instance named **b**, and configure an RD and route targets for the VPN instance.

```
[PE2] ip vpn-instance b
[PE2-vpn-instance-b] route-distinguisher 200:1
[PE2-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE2-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE2-vpn-instance-b] quit
```

Enable IP multicast routing for VPN instance **b**.

```
[PE2] multicast routing vpn-instance b
[PE2-mrib-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE2] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv4 address family for VPN instance **b**.

```
[PE2-mvpn-b] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE2-mvpn-b-ipv4] default-group 239.2.2.2
[PE2-mvpn-b-ipv4] source loopback 1
[PE2-mvpn-b-ipv4] data-group 225.4.4.0 28
[PE2-mvpn-b-ipv4] quit
[PE2-mvpn-b] quit
```

Create a VPN instance named **a**, and configure an RD and route targets for VPN instance.

```
[PE2] ip vpn-instance a
[PE2-vpn-instance-a] route-distinguisher 100:1
[PE2-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE2-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE2-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE2] multicast routing vpn-instance a
[PE2-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE2] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 address family for VPN instance **a**.

```
[PE2-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE2-mvpn-a-ipv4] default-group 239.1.1.1
[PE2-mvpn-a-ipv4] source loopback 1
[PE2-mvpn-a-ivp4] data-group 225.2.2.0 28
[PE2-mvpn-a-ipv4] quit
[PE2-mvpn-a] quit
```

Assign an IP address to VLAN-interface 15.

```
[PE2] interface vlan-interface 15
[PE2-Vlan-interface15] ip address 192.168.7.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 15.

```
[PE2-Vlan-interface15] pim sm
[PE2-Vlan-interface15] mpls enable
[PE2-Vlan-interface15] mpls ldp enable
[PE2-Vlan-interface15] quit
```

Associate VLAN-interface 13 with VPN instance **b**, assign an IP address to VLAN-interface 13, and enable PIM-SM on the interface.

```
[PE2] interface vlan-interface 13
[PE2-Vlan-interface13] ip binding vpn-instance b
[PE2-Vlan-interface13] ip address 10.110.3.1 24
[PE2-Vlan-interface13] pim sm
[PE2-Vlan-interface13] quit
```

Associate VLAN-interface 14 with VPN instance **a**.

```
[PE2] interface vlan-interface 14
[PE2-Vlan-interface14] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 14, and enable PIM-SM on the interface.

```
[PE2-Vlan-interface14] ip address 10.110.4.1 24
[PE2-Vlan-interface14] pim sm
[PE2-Vlan-interface14] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

Configure BGP.

```
[PE2] bgp 100
[PE2-bgp-default] group vpn-g internal
[PE2-bgp-default] peer vpn-g connect-interface loopback 1
[PE2-bgp-default] peer 1.1.1.1 group vpn-g
[PE2-bgp-default] peer 1.1.1.3 group vpn-g
[PE2–bgp-default] ip vpn-instance a
[PE2-bgp-default-a] address-family ipv4
[PE2-bgp-default-ipv4-a] import-route rip 2
[PE2-bgp-default-ipv4-a] import-route direct
[PE2-bgp-default-ipv4-a] quit
[PE2-bgp-default-a] quit
[PE2–bgp-default] ip vpn-instance b
[PE2-bgp-default-b] address-family ipv4
[PE2-bgp-default-ipv4-b] import-route rip 3
[PE2-bgp-default-ipv4-b] import-route direct
```

```
[PE2-bgp-default-ipv4-b] quit
[PE2-bgp-default-b] quit
[PE2–bgp-default] address-family vpnv4
[PE2–bgp-default-vpnv4] peer vpn-g enable
[PE2–bgp-default-vpnv4] quit
[PE2–bgp-default] quit
```

Configure OSPF.

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 192.168.7.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configure RIP.

```
[PE2] rip 2 vpn-instance a
[PE2-rip-2] network 10.110.4.0 0.0.0.255
[PE2-rip-2] import-route bgp
[PE2-rip-2] quit
[PE2] rip 3 vpn-instance b
[PE2-rip-3] network 10.110.3.0 0.0.0.255
[PE2-rip-3] import-route bgp
[PE2-rip-3] return
```

3. Configure PE 3:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing
[PE3-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE3] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 17, VLAN 18, or VLAN 19.

```
[PE3] interface gigabitethernet 1/0/4
[PE3-GigabitEthernet1/0/4] port service-loopback group 1
[PE3-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

Create a VPN instance named **a**, and configure an RD and route targets for the VPN instance.

```
[PE3] ip vpn-instance a
[PE3-vpn-instance-a] route-distinguisher 100:1
[PE3-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE3-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE3-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE3] multicast routing vpn-instance a
[PE3-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE3] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 address family for VPN instance **a**.

```
[PE3-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE3-mvpn-a-ipv4] default-group 239.1.1.1
[PE3-mvpn-a-ipv4] source loopback 1
[PE3-mvpn-a-ipv4] data-group 225.2.2.0 28
[PE3-mvpn-a-ipv4] quit
[PE3-mvpn-a] quit
```

Create a VPN instance named **b**, and configure an RD and route targets for the VPN instance.

```
[PE3] ip vpn-instance b
[PE3-vpn-instance-b] route-distinguisher 200:1
[PE3-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE3-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE3-vpn-instance-b] quit
```

Enable IP multicast routing for VPN instance **b**.

```
[PE3] multicast routing vpn-instance b
[PE3-mrib-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE3] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv4 address family for VPN instance **b**.

```
[PE3-mvpn-b] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE3-mvpn-b-ipv4] default-group 239.2.2.2
[PE3-mvpn-b-ipv4] source loopback 1
[PE3-mvpn-b-ipv4] data-group 225.4.4.0 28
[PE3-mvpn-b-ipv4] quit
[PE3-mvpn-b] quit
```

Assign an IP address to VLAN-interface 19.

```
[PE3] interface vlan-interface 19
[PE3-Vlan-interface19] ip address 192.168.8.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 19.

```
[PE3-Vlan-interface19] pim sm
[PE3-Vlan-interface19] mpls enable
[PE3-Vlan-interface19] mpls ldp enable
[PE3-Vlan-interface19] quit
```

Associate VLAN-interface 17 with VPN instance **a**.

```
[PE3] interface vlan-interface 17
[PE3-Vlan-interface17] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 17, and enable PIM-SM on the interface.

```
[PE3-Vlan-interface17] ip address 10.110.5.1 24
[PE3-Vlan-interface17] pim sm
[PE3-Vlan-interface17] quit
```

Associate VLAN-interface 18 with VPN instance **b**.

```
[PE3] interface vlan-interface 18
```

```
[PE3-Vlan-interface18] ip binding vpn-instance b
```

Assign an IP address to VLAN-interface 18, and enable PIM-SM on the interface.

```
[PE3-Vlan-interface18] ip address 10.110.6.1 24
[PE3-Vlan-interface18] pim sm
[PE3-Vlan-interface18] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

Associate Loopback 2 with VPN instance **b**.

```
[PE3] interface loopback 2
[PE3-LoopBack2] ip binding vpn-instance b
```

Assign an IP address to Loopback 2, and enable PIM-SM on the interface.

```
[PE3-LoopBack2] ip address 33.33.33.33 32
[PE3-LoopBack2] pim sm
[PE3-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[PE3] pim vpn-instance b
[PE3-pim-b] c-bsr 33.33.33.33
[PE3-pim-b] c-rp 33.33.33.33
[PE3-pim-b] quit
```

Configure BGP.

```
[PE3] bgp 100
[PE3-bgp-default] group vpn-g internal
[PE3-bgp-default] peer vpn-g connect-interface loopback 1
[PE3-bgp-default] peer 1.1.1.1 group vpn-g
[PE3-bgp-default] peer 1.1.1.2 group vpn-g
[PE3–bgp-default] ip vpn-instance a
[PE3-bgp-default-a] address-family ipv4
[PE3-bgp-default-ipv4-a] import-route rip 2
[PE3-bgp-default-ipv4-a] import-route direct
[PE3-bgp-default-ipv4-a] quit
[PE3-bgp-default-a] quit
[PE3–bgp-default] ip vpn-instance b
[PE3-bgp-default-b] address-family ipv4
[PE3-bgp-default-ipv4-b] import-route rip 3
[PE3-bgp-default-ipv4-b] import-route direct
[PE3-bgp-default-ipv4-b] quit
[PE3-bgp-default-b] quit
[PE3–bgp-default] address-family vpnv4
[PE3–bgp-default-vpnv4] peer vpn-g enable
[PE3–bgp-default-vpnv4] quit
[PE3–bgp-default] quit
```

Configure OSPF.

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
```

```
[PE3-ospf-1-area-0.0.0.0] network 192.168.8.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

Configure RIP.

```
[PE3] rip 2 vpn-instance a
[PE3-rip-2] network 10.110.5.0 0.0.0.255
[PE3-rip-2] import-route bgp
[PE3-rip-2] quit
[PE3] rip 3 vpn-instance b
[PE3-rip-3] network 10.110.6.0 0.0.0.255
[PE3-rip-3] network 33.33.33.33 0.0.0.0
[PE3-rip-3] import-route bgp
[PE3-rip-3] return
```

4. Configure P:

Enable IP multicast routing on the public network.

```
<P> system-view
[P] multicast routing
[P-mrib] quit
```

Configure an MPLS LSR ID, and enable LDP globally.

```
[P] mpls lsr-id 2.2.2.2
[P] mpls ldp
[P-ldp] quit
```

Assign an IP address to VLAN-interface 12.

```
[P] interface vlan-interface 12
[P-Vlan-interface12] ip address 192.168.6.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 12.

```
[P-Vlan-interface12] pim sm
[P-Vlan-interface12] mpls enable
[P-Vlan-interface12] mpls ldp enable
[P-Vlan-interface12] quit
```

Assign an IP address to VLAN-interface 15.

```
[P] interface vlan-interface 15
[P-Vlan-interface15] ip address 192.168.7.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 15.

```
[P-Vlan-interface15] pim sm
[P-Vlan-interface15] mpls enable
[P-Vlan-interface15] mpls ldp enable
[P-Vlan-interface15] quit
```

Assign an IP address to VLAN-interface 19.

```
[P] interface vlan-interface 19
[P-Vlan-interface19] ip address 192.168.8.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 19.

```
[P-Vlan-interface19] pim sm
[P-Vlan-interface19] mpls enable
[P-Vlan-interface19] mpls ldp enable
[P-Vlan-interface19] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[P] interface loopback 1
[P-LoopBack1] ip address 2.2.2.2 32
[P-LoopBack1] pim sm
[P-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[P] pim
[P-pim] c-bsr 2.2.2.2
[P-pim] c-rp 2.2.2.2
[P-pim] quit
```

Configure OSPF.

```
[P] ospf 1
[P-ospf-1] area 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 192.168.6.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.168.7.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.168.8.0 0.0.0.255
```

5. Configure CE a1:

Enable IP multicast routing.

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
```

Assign an IP address to VLAN-interface 10, and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.110.7.1 24
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
```

Assign an IP address to VLAN-interface 11, and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.110.2.2 24
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
```

Configure RIP.

```
[CEa1] rip 2
[CEa1-rip-2] network 10.110.2.0 0.0.0.255
[CEa1-rip-2] network 10.110.7.0 0.0.0.255
```

6. Configure CE b1:

Enable IP multicast routing.

```
<CEb1> system-view
[CEb1] multicast routing
[CEb1-mrib] quit
```

Assign an IP address to VLAN-interface 30, and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 30
[CEb1-Vlan-interface30] ip address 10.110.8.1 24
[CEb1-Vlan-interface30] pim sm
[CEb1-Vlan-interface30] quit
```

Assign an IP address to VLAN-interface 13, and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 13
```

```
[CEb1-Vlan-interface13] ip address 10.110.3.2 24
[CEb1-Vlan-interface13] pim sm
[CEb1-Vlan-interface13] quit
```

Configure RIP.

```
[CEb1] rip 3
[CEb1-rip-3] network 10.110.3.0 0.0.0.255
[CEb1-rip-3] network 10.110.8.0 0.0.0.255
```

7. Configure CE a2:

Enable IP multicast routing.

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
```

Assign an IP address to VLAN-interface 40, and enable IGMP on the interface.

```
[CEa2] interface vlan-interface 40
[CEa2-Vlan-interface40] ip address 10.110.9.1 24
[CEa2-Vlan-interface40] igmp enable
[CEa2-Vlan-interface40] quit
```

Assign an IP address to VLAN-interface 14, and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 14
[CEa2-Vlan-interface14] ip address 10.110.4.2 24
[CEa2-Vlan-interface14] pim sm
[CEa2-Vlan-interface14] quit
```

Assign an IP address to VLAN-interface 16, and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 16
[CEa2-Vlan-interface16] ip address 10.110.12.1 24
[CEa2-Vlan-interface16] pim sm
[CEa2-Vlan-interface16] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[CEa2] interface loopback 1
[CEa2-LoopBack1] ip address 22.22.22.22 32
[CEa2-LoopBack1] pim sm
[CEa2-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[CEa2] pim
[CEa2-pim] c-bsr 22.22.22.22
[CEa2-pim] c-rp 22.22.22.22
[CEa2-pim] quit
```

Configure RIP.

```
[CEa2] rip 2
[CEa2-rip-2] network 10.110.4.0 0.0.0.255
[CEa2-rip-2] network 10.110.9.0 0.0.0.255
[CEa2-rip-2] network 10.110.12.0 0.0.0.255
[CEa2-rip-2] network 22.22.22.22 0.0.0.0
```

8. Configure CE a3:

Enable IP multicast routing.

```
<CEa3> system-view
[CEa3] multicast routing
```

```
[CEa3-mrib] quit
```

Assign an IP address to VLAN-interface 50, and enable IGMP on the interface.

```
[CEa3] interface vlan-interface 50
[CEa3-Vlan-interface50] ip address 10.110.10.1 24
[CEa3-Vlan-interface50] igmp enable
[CEa3-Vlan-interface50] quit
```

Assign an IP address to VLAN-interface 17, and enable PIM-SM on the interface.

```
[CEa3] interface vlan-interface 17
[CEa3-Vlan-interface17] ip address 10.110.5.2 24
[CEa3-Vlan-interface17] pim sm
[CEa3-Vlan-interface17] quit
```

Assign an IP address to VLAN-interface 16, and enable PIM-SM on the interface.

```
[CEa3] interface vlan-interface 16
[CEa3-Vlan-interface16] ip address 10.110.12.2 24
[CEa3-Vlan-interface16] pim sm
[CEa3-Vlan-interface16] quit
```

Configure RIP.

```
[CEa3] rip 2
[CEa3-rip-2] network 10.110.5.0 0.0.0.255
[CEa3-rip-2] network 10.110.10.0 0.0.0.255
[CEa3-rip-2] network 10.110.12.0 0.0.0.255
```

9. Configure CE b2:

Enable IP multicast routing.

```
<CEb2> system-view
[CEb2] multicast routing
[CEb2-mrib] quit
```

Assign an IP address to VLAN-interface 60, and enable IGMP on the interface.

```
[CEb2] interface vlan-interface 60
[CEb2-Vlan-interface60] ip address 10.110.11.1 24
[CEb2-Vlan-interface60] igmp enable
[CEb2-Vlan-interface60] quit
```

Assign an IP address to VLAN-interface 18, and enable PIM-SM on the interface.

```
[CEb2] interface vlan-interface 18
[CEb2-Vlan-interface18] ip address 10.110.6.2 24
[CEb2-Vlan-interface18] pim sm
[CEb2-Vlan-interface18] quit
```

Configure RIP.

```
[CEb2] rip 3
[CEb2-rip-3] network 10.110.6.0 0.0.0.255
[CEb2-rip-3] network 10.110.11.0 0.0.0.255
```

Verifying the configuration

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 1.

```
[PE1] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      a
```

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 2.

```
[PE2] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.2          MTunnel0      a
 239.1.1.1        1.1.1.2          MTunnel1      b
```

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 3.

```
[PE3] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.3          MTunnel0      a
 239.2.2.2        1.1.1.3          MTunnel1      b
```

Example: Configuring intra-AS M6VPE

Network configuration

As shown in Figure 12, configure intra-AS M6VPE to meet the following requirements:

Item	Network configuration
Multicast sources and receivers	• In VPN instance **a**, S 1 is an IPv6 multicast source, and R 1, R 2, and R 3 are receivers. • In VPN instance **b**, S 2 is an IPv6 multicast source, and R 4 is a receiver. • For VPN instance **a**, the default group is 239.1.1.1, and the data group range is 225.2.2.0 to 225.2.2.15. • For VPN instance **b**, the default group is 239.2.2.2, and the data group range is 225.4.4.0 to 225.4.4.15.
VPN instances to which PE interfaces belong	• PE 1: VLAN-interface 11 and VLAN-interface 20 belong to VPN instance **a**. VLAN-interface 12 and Loopback 1 belong to the public network. • PE 2: VLAN-interface 13 belongs to VPN instance **b**. VLAN-interface 14 belongs to VPN instance **a**. VLAN-interface 15 and Loopback 1 belong to the public network. • PE 3: VLAN-interface 17 belongs to VPN instance **a**. VLAN-interface 18 and Loopback 2 belongs to VPN instance **b**. VLAN-interface 19 and Loopback 1 belong to the public network.
Unicast routing protocols and MPLS	• Configure OSPF on the public network, and configure OSPFv3 between the PEs and the CEs. • Establish BGP peer connections between PE 1, PE 2, and PE 3 on their respective Loopback 1. • Configure MPLS on the public network.
IP multicast routing and IPv6 multicast routing	• Enable IP multicast routing on P. • Enable IP multicast routing for the public network on PE 1, PE 2, and PE 3. • Enable IPv6 multicast routing for VPN instance **a** on PE 1, PE 2, and PE 3. • Enable IPv6 multicast routing for VPN instance **b** on PE 2 and PE 3. • Enable IPv6 multicast routing on CE a1, CE a2, CE a3, CE b1, and CE b2.
MLDv1	• Enable MLDv1 on VLAN-interface 20 of PE 1.

Item	Network configuration
	• Enable MLDv1 on VLAN-interface 40 of CE a2. • Enable MLDv1 on VLAN-interface 50 of CE a3. • Enable MLDv1 on VLAN-interface 60 of CE b2.
PIM and IPv6 PIM	Enable PIM-SM on the public network and IPv6 PIM-SM for VPN instances **a** and **b**: • Enable PIM-SM on all interfaces of P. • Enable PIM-SM on all public network interfaces and IPv6 PIM-SM on private network interfaces of PE 1, PE 2, and PE 3. • Enable IPv6 PIM-SM on all interfaces that do not have attached receivers on CE a1, CE a2, CE a3, CE b1, and CE b2. • Configure Loopback 1 of P as a C-BSR and a C-RP for the public network to provide services for all IPv4 multicast groups. • Configure Loopback 1 of CE a2 as a C-BSR and a C-RP for VPN instance **a** to provide services for all IPv6 multicast groups. • Configure Loopback 2 of PE 3 as a C-BSR and a C-RP for VPN instance **b** to provide services for all IPv6 multicast groups.

Figure 12 Network diagram

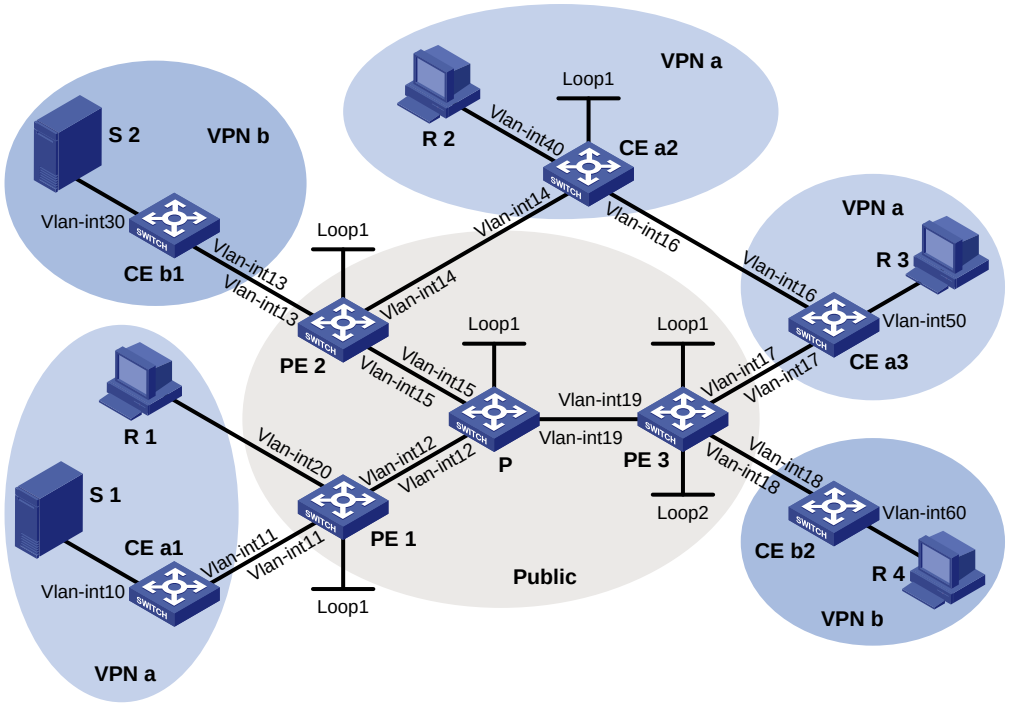


Table 4 Interface and IP address assignment

Device	Interface	IPv4/IPv6 address	Device	Interface	IPv4/IPv6 address
S 1	—	10:110:7::2/64	PE 3	Vlan-int19	192.168.8.1/24
S 2	—	10:110:8::2/64	PE 3	Vlan-int17	10:110:5::1/64
R 1	—	10:110:1::2/64	PE 3	Vlan-int18	10:110:6::1/64
R 2	—	10:110:9::2/64	PE 3	Loop1	1.1.1.3/32
R 3	—	10:110:10::2/64	PE 3	Loop2	33:33:33::33/128

Device	Interface	IPv4/IPv6 address	Device	Interface	IPv4/IPv6 address
R 4	—	10:110:11::2/64	CE a1	Vlan-int10	10:110:7::1/64
P	Vlan-int12	192.168.6.2/24	CE a1	Vlan-int11	10:110:2::2/64
P	Vlan-int15	192.168.7.2/24	CE a2	Vlan-int40	10:110:9::1/64
P	Vlan-int19	192.168.8.2/24	CE a2	Vlan-int14	10:110:4::2/64
P	Loop1	2.2.2.2/32	CE a2	Vlan-int16	10:110:12::1/64
PE 1	Vlan-int12	192.168.6.1/24	CE a2	Loop1	22:22:22::22/128
PE 1	Vlan-int20	10:110:1::1/64	CE a3	Vlan-int50	10:110:10::1/64
PE 1	Vlan-int11	10:110:2::1/64	CE a3	Vlan-int17	10:110:5::2/64
PE 1	Loop1	1.1.1.1/32	CE a3	Vlan-int16	10:110:12::2/64
PE 2	Vlan-int15	192.168.7.1/24	CE b1	Vlan-int30	10:110:8::1/64
PE 2	Vlan-int13	10:110:3::1/64	CE b1	Vlan-int13	10:110:3::2/64
PE 2	Vlan-int14	10:110:4::1/64	CE b2	Vlan-int60	10:110:11::1/64
PE 2	Loop1	1.1.1.2/32	CE b2	Vlan-int18	10:110:6::2/64

Procedure

1. Configure PE 1:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
[PE1-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 11, VLAN 12, or VLAN 20.

```
[PE1] interface gigabitethernet 1/0/4
[PE1-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
```

Create a VPN instance named **a**, and configure the RD and route targets for the VPN instance.

```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] quit
```

Enable IPv6 multicast routing for VPN instance **a**.

```
[PE1] ipv6 multicast routing vpn-instance a
[PE1-mrib6-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE1] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv6 address family for VPN instance **a**.

```
[PE1-mvpn-a] address-family ipv6
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE1-mvpn-a-ipv6] default-group 239.1.1.1
[PE1-mvpn-a-ipv6] source loopback 1
[PE1-mvpn-a-ipv6] data-group 225.2.2.0 28
[PE1-mvpn-a-ipv6] quit
[PE1-mvpn-a] quit
```

Assign an IP address to VLAN-interface 12.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip address 192.168.6.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 12.

```
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] mpls enable
[PE1-Vlan-interface12] mpls ldp enable
[PE1-Vlan-interface12] quit
```

Associate VLAN-interface 20 with VPN instance **a**, and assign an IPv6 address to the interface.

```
[PE1] interface vlan-interface 20
[PE1-Vlan-interface20] ip binding vpn-instance a
[PE1-Vlan-interface20] ipv6 address 10:110:1::1 64
```

Configure VLAN-interface 20 to run OSPFv3 process 2 in Area 0, and enable MLD on the interface.

```
[PE1-Vlan-interface20] ospfv3 2 area 0.0.0.0
[PE1-Vlan-interface20] mld enable
[PE1-Vlan-interface20] quit
```

Associate VLAN-interface 11 with VPN instance **a**, and assign an IPv6 address to the interface.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance a
[PE1-Vlan-interface11] ipv6 address 10:110:2::1 64
```

Configure VLAN-interface 11 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[PE1-Vlan-interface11] ospfv3 2 area 0.0.0.0
[PE1-Vlan-interface11] ipv6 pim sm
[PE1-Vlan-interface11] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

Configure BGP.

```
[PE1] bgp 100
[PE1-bgp-default] group vpn-g internal
[PE1-bgp-default] peer vpn-g connect-interface loopback 1
```

```
[PE1-bgp-default] peer 1.1.1.2 group vpn-g
[PE1-bgp-default] peer 1.1.1.3 group vpn-g
[PE1–bgp-default] ip vpn-instance a
[PE1-bgp-default-a] address-family ipv6
[PE1-bgp-default-ipv6-a] import-route ospfv3 2
[PE1-bgp-default-ipv6-a] import-route direct
[PE1-bgp-default-ipv6-a] quit
[PE1-bgp-default-a] quit
[PE1–bgp-default] address-family vpnv6
[PE1–bgp-default-vpnv6] peer vpn-g enable
[PE1–bgp-default-vpnv6] quit
[PE1–bgp-default] quit
```

Configure OSPF.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 192.168.6.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

Configure OSPFv3.

```
[PE1] ospfv3 2 vpn-instance a
[PE1-ospfv3-2] router-id 1.1.1.1
[PE1-ospfv3-2] import-route bgp4+
[PE1-ospfv3-2] import-route direct
[PE1-ospfv3-2] area 0
[PE1-ospfv3-2-area-0.0.0.0] return
```

2. Configure PE 2:

Configure a global RD, and enable IP multicast routing on the public network.

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing
[PE2-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE2] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 13, VLAN 14, or VLAN 15.

```
[PE2] interface gigabitethernet 1/0/4
[PE2-GigabitEthernet1/0/4] port service-loopback group 1
[PE2-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls ldp
[PE2-ldp] quit
```

Create a VPN instance named **b**, and configure the RD and route targets for the VPN instance.

```
[PE2] ip vpn-instance b
[PE2-vpn-instance-b] route-distinguisher 200:1
[PE2-vpn-instance-b] vpn-target 200:1 export-extcommunity
```

```
[PE2-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE2-vpn-instance-b] quit
```

Enable IPv6 multicast routing for VPN instance **b**.

```
[PE2] ipv6 multicast routing vpn-instance b
[PE2-mrib6-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE2] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv6 address family for VPN instance **b**.

```
[PE2-mvpn-b] address-family ipv6
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE2-mvpn-b-ipv6] default-group 239.2.2.2
[PE2-mvpn-b-ipv6] source loopback 1
[PE2-mvpn-b-ipv6] data-group 225.4.4.0 28
[PE2-mvpn-b-ipv6] quit
[PE2-mvpn-b] quit
```

Create a VPN instance named **a**, and configure the RD and route targets for the VPN instance.

```
[PE2] ip vpn-instance a
[PE2-vpn-instance-a] route-distinguisher 100:1
[PE2-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE2-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE2-vpn-instance-a] quit
```

Enable IPv6 multicast routing for VPN instance **a**.

```
[PE2] ipv6 multicast routing vpn-instance a
[PE2-mrib6-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE2] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv6 address family for VPN instance **a**.

```
[PE2-mvpn-a] address-family ipv6
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE2-mvpn-a-ipv6] default-group 239.1.1.1
[PE2-mvpn-a-ipv6] source loopback 1
[PE2-mvpn-a-ipv6] data-group 225.2.2.0 28
[PE2-mvpn-a-ipv6] quit
[PE2-mvpn-a] quit
```

Assign an IP address to VLAN-interface 15.

```
[PE2] interface vlan-interface 15
[PE2-Vlan-interface15] ip address 192.168.7.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 15.

```
[PE2-Vlan-interface15] pim sm
[PE2-Vlan-interface15] mpls enable
[PE2-Vlan-interface15] mpls ldp enable
[PE2-Vlan-interface15] quit
```

Associate VLAN-interface 13 with VPN instance **b**, and assign an IPv6 address to the interface.

```
[PE2] interface vlan-interface 13
```

```
[PE2-Vlan-interface13] ip binding vpn-instance b
[PE2-Vlan-interface13] ipv6 address 10:110:3::1 64
```

Configure VLAN-interface 13 to run OSPFv3 process 3 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[PE2-Vlan-interface13] ospfv3 3 area 0.0.0.0
[PE2-Vlan-interface13] ipv6 pim sm
[PE2-Vlan-interface13] quit
```

Associate VLAN-interface 14 with VPN instance **a**, and assign an IPv6 address to the interface.

```
[PE2] interface vlan-interface 14
[PE2-Vlan-interface14] ip binding vpn-instance a
[PE2-Vlan-interface14] ipv6 address 10:110::4::1 64
```

Configure VLAN-interface 14 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[PE2-Vlan-interface14] ospfv3 2 area 0.0.0.0
[PE2-Vlan-interface14] ipv6 pim sm
[PE2-Vlan-interface14] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

Configure BGP.

```
[PE2] bgp 100
[PE2-bgp-default] group vpn-g internal
[PE2-bgp-default] peer vpn-g connect-interface loopback 1
[PE2-bgp-default] peer 1.1.1.1 group vpn-g
[PE2-bgp-default] peer 1.1.1.3 group vpn-g
[PE2–bgp-default] ip vpn-instance a
[PE2-bgp-default-a] address-family ipv6
[PE2-bgp-default-ipv6-a] import-route ospfv3 2
[PE2-bgp-default-ipv6-a] import-route direct
[PE2-bgp-default-ipv6-a] quit
[PE2-bgp-default-a] quit
[PE2–bgp-default] ip vpn-instance b
[PE2-bgp-default-b] address-family ipv6
[PE2-bgp-default-ipv6-b] import-route ospfv3 3
[PE2-bgp-default-ipv6-b] import-route direct
[PE2-bgp-default-ipv6-b] quit
[PE2-bgp-default-b] quit
[PE2–bgp-default] address-family vpnv6
[PE2–bgp-default-vpnv6] peer vpn-g enable
[PE2–bgp-default-vpnv6] quit
[PE2–bgp-default] quit
```

Configure OSPF.

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
```

```
[PE2-ospf-1-area-0.0.0.0] network 192.168.7.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

Configure OSPFv3.

```
[PE2] ospfv3 2 vpn-instance a
[PE2-ospfv3-2] router-id 2.2.2.2
[PE2-ospfv3-2] import-route bgp4+
[PE2-ospfv3-2] import-route direct
[PE2-ospfv3-2] area 0
[PE2-ospfv3-2-area-0.0.0.0] quit
[PE2] ospfv3 3 vpn-instance b
[PE2-ospfv3-3] router-id 3.3.3.3
[PE2-ospfv3-3] import-route bgp4+
[PE2-ospfv3-3] import-route direct
[PE2-ospfv3-3] area 0
```

3. Configure PE 3:

Configure a global RD, and enable IP multicast routing on the public network.

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing
[PE3-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE3] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 17, VLAN 18, or VLAN 19.

```
[PE3] interface gigabitethernet 1/0/4
[PE3-GigabitEthernet1/0/4] port service-loopback group 1
[PE3-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

Create a VPN instance named **a**, and configure the RD and route targets for the VPN instance.

```
[PE3] ip vpn-instance a
[PE3-vpn-instance-a] route-distinguisher 100:1
[PE3-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE3-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE3-vpn-instance-a] quit
```

Enable IPv6 multicast routing for VPN instance **a**.

```
[PE3] ipv6 multicast routing vpn-instance a
[PE3-mrib6-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE3] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv6 address family for VPN instance **a**.

```
[PE3-mvpn-a] address-family ipv6
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE3-mvpn-a-ipv6] default-group 239.1.1.1
[PE3-mvpn-a-ipv6] source loopback 1
[PE3-mvpn-a-ipv6] data-group 225.2.2.0 28
[PE3-mvpn-a-ipv6] quit
[PE3-mvpn-a] quit
```

Create a VPN instance named **b**, and configure the RD and route targets for the VPN instance.

```
[PE3] ip vpn-instance b
[PE3-vpn-instance-b] route-distinguisher 200:1
[PE3-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE3-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE3-vpn-instance-b] quit
```

Enable IPv6 multicast routing for VPN instance **b**.

```
[PE3] ipv6 multicast routing vpn-instance b
[PE3-mrib6-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE3] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv6 address family for VPN instance **a**.

```
[PE3-mvpn-b] address-family ipv6
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE3-mvpn-b-ipv6] default-group 239.2.2.2
[PE3-mvpn-b-ipv6] source loopback 1
[PE3-mvpn-b-ipv6] data-group 225.4.4.0 28
[PE3-mvpn-b-ipv6] quit
[PE3-mvpn-b] quit
```

Assign an IP address to VLAN-interface 19.

```
[PE3] interface vlan-interface 19
[PE3-Vlan-interface19] ip address 192.168.8.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 19.

```
[PE3-Vlan-interface19] pim sm
[PE3-Vlan-interface19] mpls enable
[PE3-Vlan-interface19] mpls ldp enable
[PE3-Vlan-interface19] quit
```

Associate VLAN-interface 17 with VPN instance **a**, and assign an IPv6 address to the interface.

```
[PE3] interface vlan-interface 17
[PE3-Vlan-interface17] ip binding vpn-instance a
[PE3-Vlan-interface17] ipv6 address 10:110:5::1 64
```

Configure VLAN-interface 17 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[PE3-Vlan-interface17] ospfv3 2 area 0.0.0.0
[PE3-Vlan-interface17] ipv6 pim sm
[PE3-Vlan-interface17] quit
```

Associate VLAN-interface 18 with VPN instance **b**, and assign an IPv6 address to the interface.

```
[PE3] interface vlan-interface 18
[PE3-Vlan-interface18] ip binding vpn-instance b
```

```
[PE3-Vlan-interface18] ipv6 address 10:110:6::1 64
```

Configure VLAN-interface 18 to run OSPFv3 process 3 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[PE3-Vlan-interface18] ospfv3 3 area 0.0.0.0
[PE3-Vlan-interface18] ipv6 pim sm
[PE3-Vlan-interface18] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

Associate Loopback 2 with VPN instance **b**, and assign an IPv6 address to the interface.

```
[PE3] interface loopback 2
[PE3-LoopBack2] ip binding vpn-instance b
[PE3-LoopBack2] ipv6 address 33:33:33::33 128
```

Configure Loopback 2 to run OSPFv3 process 3 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[PE3-LoopBack2] ospfv3 3 area 0.0.0.0
[PE3-LoopBack2] ipv6 pim sm
[PE3-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[PE3] ipv6 pim vpn-instance b
[PE3-pim6-b] c-bsr 33:33:33::33
[PE3-pim6-b] c-rp 33:33:33::33
[PE3-pim6-b] quit
```

Configure BGP.

```
[PE3] bgp 100
[PE3-bgp-default] group vpn-g internal
[PE3-bgp-default] peer vpn-g connect-interface loopback 1
[PE3-bgp-default] peer 1.1.1.1 group vpn-g
[PE3-bgp-default] peer 1.1.1.2 group vpn-g
[PE3–bgp-default] ip vpn-instance a
[PE3-bgp-default-a] address-family ipv6
[PE3-bgp-default-ipv6-a] import-route ospfv3 2
[PE3-bgp-default-ipv6-a] import-route direct
[PE3-bgp-default-ipv6-a] quit
[PE3-bgp-default-a] quit
[PE3–bgp-default] ip vpn-instance b
[PE3-bgp-default-b] address-family ipv6
[PE3-bgp-default-ipv6-b] import-route ospfv3 3
[PE3-bgp-default-ipv6-b] import-route direct
[PE3-bgp-default-ipv6-b] quit
[PE3-bgp-default-b] quit
[PE3–bgp-default] address-family vpnv6
[PE3–bgp-default-vpnv6] peer vpn-g enable
[PE3–bgp-default-vpnv6] quit
[PE3–bgp-default] quit
```

Configure OSPF.

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 192.168.8.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

Configure OSPFv3.

```
[PE3] ospfv3 2 vpn-instance a
[PE3-ospfv3-2] router-id 4.4.4.4
[PE3-ospfv3-2] import-route bgp4+
[PE3-ospfv3-2] import-route direct
[PE3-ospfv3-2]  area 0
[PE3-ospfv3-2-area-0.0.0.0] quit
[PE3] ospfv3 3 vpn-instance b
[PE3-ospfv3-3] router-id 5.5.5.5
[PE3-ospfv3-3] import-route bgp4+
[PE3-ospfv3-3] import-route direct
[PE3-ospfv3-3]  area 0
```

4. Configure P:

Enable IP multicast routing on the public network.

```
<P> system-view
[P] multicast routing
[P-mrib] quit
```

Configure an LSR ID, and enable LDP globally.

```
[P] mpls lsr-id 2.2.2.2
[P] mpls ldp
[P-ldp] quit
```

Assign an IP address to VLAN-interface 12.

```
[P] interface vlan-interface 12
[P-Vlan-interface12] ip address 192.168.6.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 12.

```
[P-Vlan-interface12] pim sm
[P-Vlan-interface12] mpls enable
[P-Vlan-interface12] mpls ldp enable
[P-Vlan-interface12] quit
```

Assign an IP address to VLAN-interface 15.

```
[P] interface vlan-interface 15
[P-Vlan-interface15] ip address 192.168.7.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 15.

```
[P-Vlan-interface15] pim sm
[P-Vlan-interface15] mpls enable
[P-Vlan-interface15] mpls ldp enable
[P-Vlan-interface15] quit
```

Assign an IP address to VLAN-interface 19.

```
[P] interface vlan-interface 19
[P-Vlan-interface19] ip address 192.168.8.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 19.

```
[P-Vlan-interface19] pim sm
[P-Vlan-interface19] mpls enable
[P-Vlan-interface19] mpls ldp enable
[P-Vlan-interface19] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[P] interface loopback 1
[P-LoopBack1] ip address 2.2.2.2 32
[P-LoopBack1] pim sm
[P-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[P] pim
[P-pim] c-bsr 2.2.2.2
[P-pim] c-rp 2.2.2.2
[P-pim] quit
```

Configure OSPF.

```
[P] ospf 1
[P-ospf-1] area 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[P-ospf-1-area-0.0.0.0] network 192.168.6.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.168.7.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.168.8.0 0.0.0.255
```

5. Configure CE a1:

Enable IPv6 multicast routing.

```
<CEa1> system-view
[CEa1] ipv6 multicast routing
[CEa1-mrib6] quit
```

Assign an IPv6 address to VLAN-interface 10.

```
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ipv6 address 10:110:7::1 64
```

Configure VLAN-interface 10 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa1-Vlan-interface10] ospfv3 2 area 0.0.0.0
[CEa1-Vlan-interface10] ipv6 pim sm
[CEa1-Vlan-interface10] quit
```

Assign an IPv6 address to VLAN-interface 11.

```
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ipv6 address 10:110:2::2 64
```

Configure VLAN-interface 11 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa1-Vlan-interface11] ospfv3 2 area 0.0.0.0
[CEa1-Vlan-interface11] ipv6 pim sm
[CEa1-Vlan-interface11] quit
```

Configure OSPFv3.

```
[CEa1] ospfv3 2
[CEa1-ospfv3-2] router-id 6.6.6.6
[CEa1-ospfv3-2] area 0
[CEa1-ospfv3-2-area-0.0.0.0] quit
```

6. Configure CE b1:

Enable IPv6 multicast routing.

```
<CEb1> system-view
[CEb1] ipv6 multicast routing
[CEb1-mrib6] quit
```

Assign an IPv6 address to VLAN-interface 30.

```
[[CEb1] interface vlan-interface 30
[CEb1-Vlan-interface30] ipv6 address 10:110:8::1 64
```

Configure VLAN-interface 30 to run OSPFv3 process 3 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEb1-Vlan-interface30] ospfv3 3 area 0.0.0.0
[CEb1-Vlan-interface30] ipv6 pim sm
[CEb1-Vlan-interface30] quit
```

Assign an IPv6 address to VLAN-interface 13.

```
[CEb1] interface vlan-interface 13
[CEb1-Vlan-interface13] ipv6 address 10:110:3::2 24
```

Configure VLAN-interface 13 to run OSPFv3 process 3 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEb1-Vlan-interface13] ospfv3 3 area 0.0.0.0
[CEb1-Vlan-interface13] ipv6 pim sm
[CEb1-Vlan-interface13] quit
```

Configure OSPFv3.

```
[CEb1] ospfv3 3
[CEb1-ospfv3-3] router-id 7.7.7.7
[CEb1-ospfv3-3] area 0
[CEb1-ospfv3-3-area-0.0.0.0] quit
```

7. Configure CE a2:

Enable IPv6 multicast routing.

```
<CEa2> system-view
[CEa2] ipv6 multicast routing
[CEa2-mrib6] quit
```

Assign an IPv6 address to VLAN-interface 40.

```
[CEa2] interface vlan-interface 40
[CEa2-Vlan-interface40] ipv6 address 10:110:9::1 64
```

Configure VLAN-interface 40 to run OSPFv3 process 2 in Area 0, and enable MLD on the interface.

```
[CEa2-Vlan-interface40] ospfv3 2 area 0.0.0.0
[CEa2-Vlan-interface40] mld enable
[CEa2-Vlan-interface40] quit
```

Assign an IPv6 address to VLAN-interface 14.

```
[CEa2] interface vlan-interface 14
[CEa2-Vlan-interface14] ipv6 address 10:110:4::2 64
```

Configure VLAN-interface 14 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa2-Vlan-interface14] ospfv3 2 area 0.0.0.0
[CEa2-Vlan-interface14] ipv6 pim sm
[CEa2-Vlan-interface14] quit
```

Assign an IPv6 address to VLAN-interface 16.

```
[CEa2] interface vlan-interface 16
```

```
[CEa2-Vlan-interface16] ipv6 address 10:110:12::1 64
```

Configure VLAN-interface 16 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa2-Vlan-interface16] ospfv3 2 area 0.0.0.0
[CEa2-Vlan-interface16] ipv6 pim sm
[CEa2-Vlan-interface16] quit
```

Assign an IPv6 address to Loopback 1.

```
[CEa2] interface loopback 1
[CEa2-LoopBack1] ipv6 address 22:22:22::22 128
```

Configure Loopback 1 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa2-LoopBack1] ospfv3 2 area 0.0.0.0
[CEa2-LoopBack1] ipv6 pim sm
[CEa2-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[CEa2] pim6
[CEa2-pim6] c-bsr 22:22:22::22
[CEa2-pim6] c-rp 22:22:22::22
[CEa2-pim6] quit
```

Configure OSPFv3.

```
[CEa2] ospfv3 2
[CEa2-ospfv3-2] router-id 8.8.8.8
[CEa2-ospfv3-2] area 0
[CEa2-ospfv3-2-area-0.0.0.0] quit
```

8. Configure CE a3:

Enable IPv6 multicast routing.

```
<CEa3> system-view
[CEa3] ipv6 multicast routing
[CEa3-mrib6] quit
```

Assign an IPv6 address to VLAN-interface 50.

```
[CEa3] interface vlan-interface 50
[CEa3-Vlan-interface50] ipv6 address 10:110:10::1 64
```

Configure VLAN-interface 50 to run OSPFv3 process 2 in Area 0, and enable MLD on the interface.

```
[CEa3-Vlan-interface50] ospfv3 2 area 0.0.0.0
[CEa3-Vlan-interface50] mld enable
[CEa3-Vlan-interface50] quit
```

Assign an IPv6 address to VLAN-interface 17.

```
[CEa3] interface vlan-interface 17
[CEa3-Vlan-interface17] ipv6 address 10:110:5::2 64
```

Configure VLAN-interface 17 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa3-Vlan-interface17] ospfv3 2 area 0.0.0.0
[CEa3-Vlan-interface17] ipv6 pim sm
[CEa3-Vlan-interface17] quit
```

Assign an IPv6 address to VLAN-interface 16.

```
[CEa3] interface vlan-interface 16
[CEa3-Vlan-interface16] ipv6 address 10:110:12::2 64
```

Configure VLAN-interface 16 to run OSPFv3 process 2 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEa3-Vlan-interface16] ospfv3 2 area 0.0.0.0
[CEa3-Vlan-interface16] ipv6 pim sm
[CEa3-Vlan-interface16] quit
```

Configure OSPFv3.

```
[CEa3] ospfv3 2
[CEa3-ospfv3-2] router-id 9.9.9.9
[CEa3-ospfv3-2] area 0
[CEa3-ospfv3-2-area-0.0.0.0] quit
```

9. Configure CE b2:

Enable IPv6 multicast routing.

```
<CEb2> system-view
[CEb2] multicast routing
[CEb2-mrib] quit
```

Assign an IPv6 address to VLAN-interface 60.

```
[CEb2] interface vlan-interface 60
[CEb2-Vlan-interface60] ipv6 address 10:110:11::1 64
```

Configure VLAN-interface 60 to run OSPFv3 process 3 in Area 0, and enable MLD on the interface.

```
[CEb2-Vlan-interface60] ospfv3 3 area 0.0.0.0
[CEb2-Vlan-interface60] mld enable
[CEb2-Vlan-interface60] quit
```

Assign an IPv6 address to VLAN-interface 18.

```
[CEb2] interface vlan-interface 18
[CEb2-Vlan-interface18] ipv6 address 10:110:6::2 64
```

Configure VLAN-interface 18 to run OSPFv3 process 3 in Area 0, and enable IPv6 PIM-SM on the interface.

```
[CEb2-Vlan-interface18] ospfv3 3 area 0.0.0.0
[CEb2-Vlan-interface18] ipv6 pim sm
[CEb2-Vlan-interface18] quit
```

Configure OSPFv3.

```
[CEb2] ospfv3 3
[CEb2-ospfv3-3] router-id 10.10.10.10
[CEb2-ospfv3-3] area 0
[CEb2-ospfv3-3-area-0.0.0.0] quit
```

Verifying the configuration

Display information about the local default group for IPv6 multicast transmission in each VPN instance on PE 1.

```
[PE1] display multicast-vpn default-group ipv6 local
MVPN local default-group information:
Group address    Source address   Interface     VPN instance
239.1.1.1        1.1.1.1          MTunnel0      a
```

Display information about the local default group for IPv6 multicast transmission in each VPN instance on PE 2.

```
[PE2] display multicast-vpn default-group ipv6 local
MVPN local default-group information:
Group address    Source address   Interface     VPN instance
```

```
239.1.1.1        1.1.1.2          MTunnel0      a
239.1.1.1        1.1.1.2          MTunnel1      b
```

Display information about the local default group for IPv6 multicast transmission in each VPN instance on PE 3.

```
[PE3] display multicast-vpn default-group ipv6 local
MVPN local default-group information:
Group address    Source address   Interface     VPN instance
239.1.1.1        1.1.1.3          MTunnel0      a
239.2.2.2        1.1.1.3          MTunnel1      b
```

Example: Configuring MDT-based MVPN inter-AS option B

Network configuration

As shown in Figure 13, configure MDT-based MVPN inter-AS option B to meet the following requirements:

Item	Network configuration
Multicast sources and receivers	• In VPN instance **a**, S 1 is a multicast source, and R 2 is a receiver. • In VPN instance **b**, S 2 is a multicast source, and R 1 is a receiver. • For VPN instance **a**, the default group is 232.1.1.1, and the data group range is 232.2.2.0 to 232.2.2.15. They are in the SSM group range. • For VPN instance **b**, the default group is 232.3.3.3, and the data group range is 232.4.4.0 to 232.4.4.15. They are in the SSM group range.
VPN instances to which PE interfaces belong	• PE 1: VLAN-interface 11 belongs to VPN instance **a**. VLAN-interface 12 belongs to VPN instance **b**. VLAN-interface 2 and Loopback 1 belong to the public network instance. • PE 2: VLAN-interface 3, VLAN-interface 4, and Loopback 1 belong to the public network instance. • PE 3: VLAN-interface 4, VLAN-interface 5, and Loopback 1 belong to the public network instance. • PE 4: VLAN-interface 13 belongs to VPN instance **a**. VLAN-interface 14 belongs to VPN instance **b**. VLAN-interface 6 and Loopback 1 belong to the public network instance.
Unicast routing protocols and MPLS	• Configure OSPF separately in AS 100 and AS 200, and configure OSPF between the PEs and CEs. • Establish IBGP peer connections between PE 1, PE 2, PE 3, and PE 4 on their respective Loopback 1. • Configure BGP MDT peer connections between PE 1, PE 2, PE 3, and PE 4 on their respective Loopback 1 and between PE 2 and PE 3 on their respective VLAN-interface 4. • Establish EBGP peer connections between VLAN-interface 4 on PE 2 and PE 3. • Configure MPLS separately in AS 100 and AS 200.
IP multicast routing	• Enable IP multicast routing on P 1 and P 2. • Enable IP multicast routing on the public network on PE 1, PE 2, PE 3, and PE 4. • Enable IP multicast routing for VPN instance **a** on PE 1 and PE 4. • Enable IP multicast routing for VPN instance **b** on PE 1 and PE 4. • Enable IP multicast routing on CE a1, CE a2, CE b1, and CE b2.
IGMP	• Enable IGMPv2 on VLAN-interface 23 of CE a2. • Enable IGMPv2 on VLAN-interface 24 of CE b2.
PIM	Enable PIM-SSM on the public network and PIM-SM on VPN instances **a** and **b**: • Enable PIM-SM on all interfaces of P 1 and P 2. • Enable PIM-SM on all public network interfaces of PE 2 and PE 3.

Item	Network configuration
	• Enable PIM-SM on all public and private network interfaces of PE 1 and PE 4. • Enable PIM-SM on all interfaces that do not have attached receiver hosts on CE a1, CE a2, CE b1, and CE b2. • Configure VLAN-interface 11 of CE a1 as a C-BSR and a C-RP for VPN instance **a** to provide services for all multicast groups. • Configure VLAN-interface 12 of CE b1 as a C-BSR and a C-RP for VPN instance **b** to provide services for all multicast groups.
RPF vector	Enable the RPF vector feature on PE 1 and PE 4.

Figure 13 Network diagram

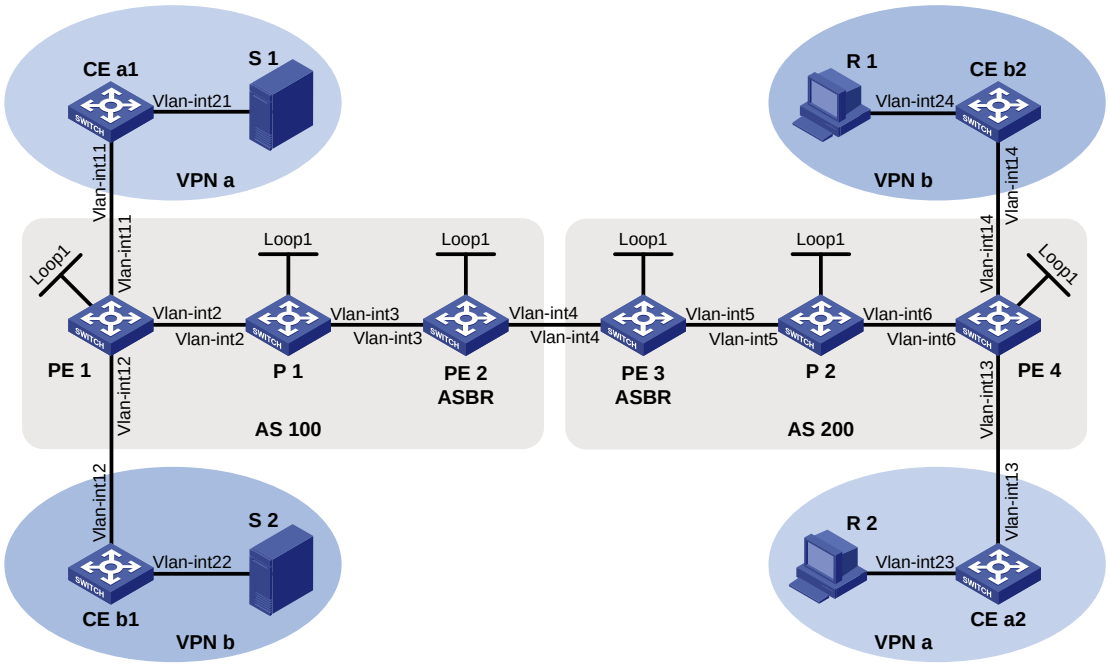


Table 5 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
S 1	—	12.1.1.100/24	R 1	—	12.4.1.100/24
S 2	—	12.2.1.100/24	R 2	—	12.3.1.100/24
PE 1	Vlan-int2	10.1.1.1/24	PE 3	Vlan-int5	10.4.1.1/24
PE 1	Vlan-int11	11.1.1.1/24	PE 3	Vlan-int4	10.3.1.2/24
PE 1	Vlan-int12	11.2.1.1/24	PE 3	Loop1	3.3.3.3/32
PE 1	Loop1	1.1.1.1/32	PE 4	Vlan-int6	10.5.1.2/24
PE 2	Vlan-int3	10.2.1.2/24	PE 4	Vlan-int13	11.3.1.1/24
PE 2	Vlan-int4	10.3.1.1/24	PE 4	Vlan-int14	11.4.1.1/24
PE 2	Loop1	2.2.2.2/32	PE 4	Loop1	4.4.4.4/24
P 1	Vlan-int2	10.1.1.2/24	P 2	Vlan-int6	10.5.1.1/24
P 1	Vlan-int3	10.2.1.1/24	P 2	Vlan-int5	10.4.1.2/24
P 1	Loop1	5.5.5.5/32	P 2	Loop1	6.6.6.6/32

Device	Interface	IP address	Device	Interface	IP address
CE a1	Vlan-int21	12.1.1.1/24	CE b1	Vlan-int22	12.2.1.1/24
CE a1	Vlan-int11	11.1.1.2/24	CE b1	Vlan-int12	11.2.1.2/24
CE a2	Vlan-int23	12.3.1.1/24	CE b2	Vlan-int24	12.4.1.1/24
CE a2	Vlan-int13	11.3.1.2/24	CE b2	Vlan-int14	11.4.1.2/24

Procedure

1. Configure PE 1:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE1> system-view
[PE1] router id 1.1.1.1
[PE1] multicast routing
[PE1-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 2, VLAN 11, or VLAN 12.

```
[PE1] interface gigabitethernet 1/0/4
[PE1-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
```

Create a VPN instance named **a**, and configure the RD and route targets for the VPN instance.

```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE1] multicast routing vpn-instance a
```

Enable the RPF vector feature.

```
[PE1-mrib-a] rpf proxy vector
[PE1-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE1] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 address family for VPN instance **a**.

```
[PE1-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE1-mvpn-a-ipv4] default-group 232.1.1.1
[PE1-mvpn-a-ipv4] source loopback 1
[PE1-mvpn-a-ipv4] data-group 232.2.2.0 28
[PE1-mvpn-a-ipv4] quit
```

```
[PE1-mvpn-a] quit
```

Create a VPN instance named **b**, and configure the RD and route targets for VPN instance.

```
[PE1] ip vpn-instance b
[PE1-vpn-instance-b] route-distinguisher 200:1
[PE1-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE1-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE1-vpn-instance-b] quit
```

Enable IP multicast routing for VPN instance **b**.

```
[PE1] multicast routing vpn-instance b
```

Enable the RPF vector feature.

```
[PE1-mrib-b] rpf proxy vector
[PE1-mrib-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE1] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv4 address family for VPN instance **b**.

```
[PE1-mvpn-b] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE1-mvpn-b-ipv4] default-group 232.3.3.3
[PE1-mvpn-b-ivp4] source loopback 1
[PE1-mvpn-b-ivp4] data-group 232.4.4.0 28
[PE1-mvpn-b-ipv4] quit
[PE1-mvpn-b] quit
```

Assign an IP address to VLAN-interface 2.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 2.

```
[PE1-Vlan-interface2] pim sm
[PE1-Vlan-interface2] mpls enable
[PE1-Vlan-interface2] mpls ldp enable
[PE1-Vlan-interface2] quit
```

Associate VLAN-interface 11 with VPN instance **a**.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 11, and enable PIM-SM on the interface.

```
[PE1-Vlan-interface11] ip address 11.1.1.1 24
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

Associate VLAN-interface 12 with VPN instance **b**.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip binding vpn-instance b
```

Assign an IP address to VLAN-interface 12, and enable PIM-SM on the interface.

```
[PE1-Vlan-interface12] ip address 11.2.1.1 24
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE1] interface loopback 1
```

```
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

Configure BGP.

```
[PE1] bgp 100
[PE1-bgp-default] peer 2.2.2.2 as-number 100
[PE1-bgp-default] peer 2.2.2.2 connect-interface loopback 1
[PE1–bgp-default] ip vpn-instance a
[PE1-bgp-default-a] address-family ipv4
[PE1-bgp-default-ipv4-a] import-route ospf 2
[PE1-bgp-default-ipv4-a] import-route direct
[PE1-bgp-default-ipv4-a] quit
[PE1-bgp-default-a] quit
[PE1–bgp-default] ip vpn-instance b
[PE1-bgp-default-b] address-family ipv4
[PE1-bgp-default-ipv4-b] import-route ospf 3
[PE1-bgp-default-ipv4-b] import-route direct
[PE1-bgp-default-ipv4-b] quit
[PE1-bgp-default-b] quit
[PE1–bgp-default] address-family vpnv4
[PE1–bgp-default-vpnv4] peer 2.2.2.2 enable
[PE1–bgp-default-vpnv4] quit
[PE1-bgp-default] address-family ipv4 mdt
[PE1-bgp-default-mdt] peer 2.2.2.2 enable
[PE1-bgp-default-mdt] quit
[PE1–bgp-default] quit
```

Configure OSPF.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
[PE1] ospf 2 vpn-instance a
[PE1-ospf-2] area 0.0.0.0
[PE1-ospf-2-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[PE1-ospf-2-area-0.0.0.0] quit
[PE1-ospf-2] quit
[PE1] ospf 3 vpn-instance b
[PE1-ospf-3] area 0.0.0.0
[PE1-ospf-3-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[PE1-ospf-3-area-0.0.0.0] quit
[PE1-ospf-3] quit
```

2. Configure PE 2:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE2> system-view
[PE2] router id 2.2.2.2
[PE2] multicast routing
```

```
[PE2-mrib] quit
```
Configure an LSR ID, and enable LDP globally.
```
[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls ldp
[PE2-ldp] quit
```
Assign an IP address to VLAN-interface 3.
```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 10.2.1.2 24
```
Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 3.
```
[PE2-Vlan-interface3] pim sm
[PE2-Vlan-interface3] mpls enable
[PE2-Vlan-interface3] mpls ldp enable
[PE2-Vlan-interface3] quit
```
Assign an IP address to VLAN-interface 4.
```
[PE2] interface vlan-interface 4
[PE2-Vlan-interface4] ip address 10.3.1.1 24
```
Enable PIM-SM and MPLS on VLAN-interface 4.
```
[PE2-Vlan-interface4] pim sm
[PE2-Vlan-interface4] mpls enable
[PE2-Vlan-interface4] quit
```
Assign an IP address to Loopback 1, and enable PIM-SM on the interface.
```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 2.2.2.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```
Configure BGP.
```
[PE2] bgp 100
[PE2-bgp-default] group 1.1.1.1 as-number 100
[PE2-bgp-default] peer 1.1.1.1 connect-interface loopback 1
[PE2-bgp-default] peer 10.3.1.2 as-number 200
[PE2-bgp-default] address-family vpnv4
[PE2-bgp-default-vpnv4] undo policy vpn-target
[PE2-bgp-default-vpnv4] peer 1.1.1.1 enable
[PE2-bgp-default-vpnv4] peer 10.3.1.2 enable
[PE2-bgp-default-vpnv4] quit
[PE2-bgp-default] address-family ipv4 mdt
[PE2-bgp-default-mdt] peer 1.1.1.1 enable
[PE2-bgp-default-mdt] peer 10.3.1.2 enable
[PE2-bgp-default-mdt] quit
[PE2–bgp-default] quit
```
Configure OSPF.
```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

3. Configure PE 3:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE3> system-view
[PE3] router id 3.3.3.3
[PE3] multicast routing
[PE3-mrib] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE3] mpls lsr-id 3.3.3.3
[PE3] mpls ldp
[PE3-ldp] quit
```

Assign an IP address to VLAN-interface 5.

```
[PE3] interface vlan-interface 5
[PE3-Vlan-interface5] ip address 10.4.1.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 5.

```
[PE3-Vlan-interface5] pim sm
[PE3-Vlan-interface5] mpls enable
[PE3-Vlan-interface5] mpls ldp enable
[PE3-Vlan-interface5] quit
```

Assign an IP address to VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] ip address 10.3.1.2 24
```

Enable PIM-SM and MPLS on VLAN-interface 4.

```
[PE3-Vlan-interface4] pim sm
[PE3-Vlan-interface4] mpls enable
[PE3-Vlan-interface4] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 3.3.3.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

Configure BGP.

```
[PE3] bgp 200
[PE3-bgp-default] group 4.4.4.4 as-number 200
[PE3-bgp-default] peer 4.4.4.4 connect-interface loopback 1
[PE3-bgp-default] peer 10.3.1.1 as-number 100
[PE3-bgp-default] address-family vpnv4
[PE3-bgp-default-vpnv4] undo policy vpn-target
[PE3-bgp-default-vpnv4] peer 4.4.4.4 enable
[PE3-bgp-default-vpnv4] peer 10.3.1.1 enable
[PE3-bgp-default-vpnv4] quit
[PE3-bgp-default] address-family ipv4 mdt
[PE3-bgp-default-mdt] peer 4.4.4.4 enable
[PE3-bgp-default-mdt] peer 10.3.1.1 enable
[PE3-bgp-default-mdt] quit
[PE3–bgp-default] quit
```

Configure OSPF.

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
```

```
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

4. Configure PE 4:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE4> system-view
[PE4] router id 4.4.4.4
[PE4] multicast routing
[PE4-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE4] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 6, VLAN 13, or VLAN 14.

```
[PE4] interface gigabitethernet 1/0/4
[PE4-GigabitEthernet1/0/4] port service-loopback group 1
[PE4-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE4] mpls lsr-id 4.4.4.4
[PE4] mpls ldp
[PE4-ldp] quit
```

Create a VPN instance named **a**, and configure the RD and route targets for the VPN instance.

```
[PE4] ip vpn-instance a
[PE4-vpn-instance-a] route-distinguisher 100:1
[PE4-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE4-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE4-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE4] multicast routing vpn-instance a
```

Enable the RPF vector feature.

```
[PE4-mrib-a] rpf proxy vector
[PE4-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE4] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 address family for VPN instance **a**.

```
[PE4-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE4-mvpn-a-ipv4] default-group 232.1.1.1
[PE4-mvpn-a-ipv4] source loopback 1
[PE4-mvpn-a-ipv4] data-group 232.2.2.0 28
[PE4-mvpn-a-ipv4] quit
[PE4-mvpn-a] quit
```

Create a VPN instance named **b**, and configure the RD and route targets for the VPN instance.

```
[PE4] ip vpn-instance b
[PE4-vpn-instance-b] route-distinguisher 200:1
```

```
[PE4-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE4-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE4-vpn-instance-b] quit
```

Enable IP multicast routing for VPN instance **b**.

```
[PE4] multicast routing vpn-instance b
```

Enable the RPF vector feature.

```
[PE4-mrib-b] rpf proxy vector
[PE4-mrib-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE4] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv4 address family for VPN instance **b**.

```
[PE4-mvpn-b] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE4-mvpn-b-ipv4] default-group 232.3.3.3
[PE4-mvpn-b-ipv4] source loopback 1
[PE4-mvpn-b-ipv4] data-group 232.4.4.0 28
[PE4-mvpn-b-ipv4] quit
[PE4-mvpn-b] quit
```

Assign an IP address to VLAN-interface 6.

```
[PE4] interface vlan-interface 6
[PE4-Vlan-interface6] ip address 10.5.1.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 6.

```
[PE4-Vlan-interface6] pim sm
[PE4-Vlan-interface6] mpls enable
[PE4-Vlan-interface6] mpls ldp enable
[PE4-Vlan-interface6] quit
```

Associate VLAN-interface 13 with VPN instance **a**.

```
[PE4] interface vlan-interface 13
[PE4-Vlan-interface13] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 13, and enable PIM-SM on the interface.

```
[PE4-Vlan-interface13] ip address 11.3.1.1 24
[PE4-Vlan-interface13] pim sm
[PE4-Vlan-interface13] quit
```

Associate VLAN-interface 14 with VPN instance **b.**

```
[PE4] interface vlan-interface 14
[PE4-Vlan-interface14] ip binding vpn-instance b
```

Assign an IP address to VLAN-interface 14, and enable PIM-SM on the interface.

```
[PE4-Vlan-interface14] ip address 11.4.1.1 24
[PE4-Vlan-interface14] pim sm
[PE4-Vlan-interface14] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE4] interface loopback 1
[PE4-LoopBack1] ip address 4.4.4.4 32
[PE4-LoopBack1] pim sm
[PE4-LoopBack1] quit
```

Configure BGP.

```
[PE4] bgp 200
[PE4-bgp-default] peer 3.3.3.3 as-number 200
[PE4-bgp-default] peer 3.3.3.3 connect-interface loopback 1
[PE4–bgp-default] ip vpn-instance a
[PE4-bgp-default-a] address-family ipv4
[PE4-bgp-default-ipv4-a] import-route ospf 2
[PE4-bgp-default-ipv4-a] import-route direct
[PE4-bgp-default-ipv4-a] quit
[PE4-bgp-default-a] quit
[PE4–bgp-default] ip vpn-instance b
[PE4-bgp-default-b] address-family ipv4
[PE4-bgp-default-ipv4-b] import-route ospf 3
[PE4-bgp-default-ipv4-b] import-route direct
[PE4-bgp-default-ipv4-b] quit
[PE4-bgp-default-b] quit
[PE4–bgp-default] address-family vpnv4
[PE4–bgp-default-vpnv4] peer 3.3.3.3 enable
[PE4–bgp-default-vpnv4] quit
[PE4-bgp-default] address-family ipv4 mdt
[PE4-bgp-default-mdt] peer 3.3.3.3 enable
[PE4-bgp-default-mdt] quit
[PE4–bgp-default] quit
```

Configure OSPF.

```
[PE4] ospf 1
[PE4-ospf-1] area 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[PE4-ospf-1-area-0.0.0.0] quit
[PE4-ospf-1] quit
[PE4] ospf 2 vpn-instance a
[PE4-ospf-2] area 0.0.0.0
[PE4-ospf-2-area-0.0.0.0] network 11.3.1.0 0.0.0.255
[PE4-ospf-2-area-0.0.0.0] quit
[PE4-ospf-2] quit
[PE4] ospf 3 vpn-instance b
[PE4-ospf-3] area 0.0.0.0
[PE4-ospf-3-area-0.0.0.0] network 11.4.1.0 0.0.0.255
[PE4-ospf-3-area-0.0.0.0] quit
[PE4-ospf-3] quit
```

5. Configure P 1:

Enable IP multicast routing on the public network.

```
<P1> system-view
[P1] multicast routing
[P1-mrib] quit
```

Configure an LSR ID, and enable LDP globally.

```
[P1] mpls lsr-id 5.5.5.5
[P1] mpls ldp
[P1-ldp] quit
```

Assign an IP address to VLAN-interface 2.

```
[P1] interface vlan-interface 2
[P1-Vlan-interface2] ip address 10.1.1.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 2.

```
[P1-Vlan-interface2] pim sm
[P1-Vlan-interface2] mpls enable
[P1-Vlan-interface2] mpls ldp enable
[P1-Vlan-interface2] quit
```

Assign an IP address to VLAN-interface 3.

```
[P1] interface vlan-interface 3
[P1-Vlan-interface3] ip address 10.2.1.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 3.

```
[P1-Vlan-interface3] pim sm
[P1-Vlan-interface3] mpls enable
[P1-Vlan-interface3] mpls ldp enable
[P1-Vlan-interface3] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[P1] interface loopback 1
[P1-LoopBack1] ip address 5.5.5.5 32
[P1-LoopBack1] pim sm
[P1-LoopBack1] quit
```

Configure OSPF.

```
[P1] ospf 1
[P1-ospf-1] area 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[P1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[P1-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
```

6. Configure P 2:

Enable IP multicast routing on the public network.

```
<P2> system-view
[P2] multicast routing
[P2-mrib] quit
```

Configure an LSR ID, and enable LDP globally.

```
[P2] mpls lsr-id 6.6.6.6
[P2] mpls ldp
[P2-ldp] quit
```

Assign an IP address to VLAN-interface 6.

```
[P2] interface vlan-interface 6
[P2-Vlan-interface6] ip address 10.5.1.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 6.

```
[P2-Vlan-interface6] pim sm
[P2-Vlan-interface6] mpls enable
[P2-Vlan-interface6] mpls ldp enable
[P2-Vlan-interface6] quit
```

Assign an IP address to VLAN-interface 5.

```
[P2] interface vlan-interface 5
[P2-Vlan-interface5] ip address 10.4.1.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 5.

```
[P2-Vlan-interface5] pim sm
[P2-Vlan-interface5] mpls enable
[P2-Vlan-interface5] mpls ldp enable
[P2-Vlan-interface5] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[P2] interface loopback 1
[P2-LoopBack1] ip address 6.6.6.6 32
[P2-LoopBack1] pim sm
[P2-LoopBack1] quit
```

Configure OSPF.

```
[P2] ospf 1
[P2-ospf-1] area 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 6.6.6.6 0.0.0.0
[P2-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[P2-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
```

7. Configure CE a1:

Enable IP multicast routing.

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
```

Assign an IP address to VLAN-interface 21, and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 21
[CEa1-Vlan-interface21] ip address 12.1.1.1 24
[CEa1-Vlan-interface21] pim sm
[CEa1-Vlan-interface21] quit
```

Assign an IP address to VLAN-interface 11, and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 11.1.1.2 24
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
```

Configure VLAN-interface 11 as a C-BSR and a C-RP.

```
[CEa1] pim
[CEa1-pim] c-bsr 11.1.1.2
[CEa1-pim] c-rp 11.1.1.2
[CEa1-pim] quit
```

Configure OSPF.

```
[CEa1] ospf 1
[CEa1-ospf-1] area 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 12.1.1.0 0.0.0.255
[CEa1-ospf-1-area-0.0.0.0] network 11.1.1.0 0.0.0.255
[CEa1-ospf-1-area-0.0.0.0] quit
[CEa1-ospf-1] quit
```

8. Configure CE b1:

Enable IP multicast routing.

```
<CEb1> system-view
[CEb1] multicast routing
```

```
[CEb1-mrib] quit
```

Assign an IP address to VLAN-interface 22, and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 22
[CEb1-Vlan-interface22] ip address 12.2.1.1 24
[CEb1-Vlan-interface22] pim sm
[CEb1-Vlan-interface22] quit
```

Assign an IP address to VLAN-interface 12, and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 12
[CEb1-Vlan-interface12] ip address 11.2.1.2 24
[CEb1-Vlan-interface12] pim sm
[CEb1-Vlan-interface12] quit
```

Configure VLAN-interface 12 as a C-BSR and a C-RP.

```
[CEb1] pim
[CEb1-pim] c-bsr 11.2.1.2 24
[CEb1-pim] c-rp 11.2.1.2 24
[CEb1-pim] quit
```

Configure OSPF.

```
[CEb1] ospf 1
[CEb1-ospf-1] area 0.0.0.0
[CEb1-ospf-1-area-0.0.0.0] network 12.2.1.0 0.0.0.255
[CEb1-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[CEb1-ospf-1-area-0.0.0.0] quit
[CEb1-ospf-1] quit
```

9. Configure CE a2:

Enable IP multicast routing.

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
```

Assign an IP address to VLAN-interface 23, and enable IGMP on the interface.

```
[CEa2] interface vlan-interface 23
[CEa2-Vlan-interface23] ip address 12.3.1.1 24
[CEa2-Vlan-interface23] igmp enable
[CEa2-Vlan-interface23] quit
```

Assign an IP address to VLAN-interface 13, and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 13
[CEa2-Vlan-interface13] ip address 11.3.1.2 24
[CEa2-Vlan-interface13] pim sm
[CEa2-Vlan-interface13] quit
```

Configure OSPF.

```
[CEa2] ospf 1
[CEa2-ospf-1] area 0.0.0.0
[CEa2-ospf-1-area-0.0.0.0] network 12.3.1.0 0.0.0.255
[CEa2-ospf-1-area-0.0.0.0] network 11.3.1.0 0.0.0.255
[CEa2-ospf-1-area-0.0.0.0] quit
[CEa2-ospf-1] quit
```

10. Configure CE b2:

Enable IP multicast routing.

```
<CEb2> system-view
[CEb2] multicast routing
[CEb2-mrib] quit
```

Assign an IP address to VLAN-interface 24, and enable IGMP on the interface.

```
[CEb2] interface vlan-interface 24
[CEb2-Vlan-interface24] ip address 12.4.1.1 24
[CEb2-Vlan-interface24] igmp enable
[CEb2-Vlan-interface24] quit
```

Assign an IP address to VLAN-interface 14, and enable PIM-SM on the interface.

```
[CEb2] interface vlan-interface 14
[CEb2-Vlan-interface14] ip address 11.4.1.2 24
[CEb2-Vlan-interface14] pim sm
[CEb2-Vlan-interface14] quit
```

Configure OSPF.

```
[CEb2] ospf 1
[CEb2-ospf-1] area 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 12.4.1.0 0.0.0.255
[CEb2-ospf-1-area-0.0.0.0] network 11.4.1.0 0.0.0.255
[CEb2-ospf-1-area-0.0.0.0] quit
[CEb2-ospf-1] quit
```

Verifying the configuration

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 1.

```
[PE1] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 232.1.1.1        1.1.1.1          MTunnel0      a
 232.3.3.3        1.1.1.1          MTunnel1      b
```

Display information about the remote default group group for IPv4 multicast transmission in each VPN instance on PE 1.

```
[PE1] display multicast-vpn default-group remote
MVPN remote default-group information:
 Group address   Source address  Next hop         VPN instance
 232.1.1.1       4.4.4.4         2.2.2.2          a
 232.3.3.3       4.4.4.4         2.2.2.2          b
```

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 4.

```
[PE4] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 232.1.1.1        4.4.4.4          MTunnel0      a
 233.3.3.3        4.4.4.4          MTunnel1      b
```

Display information about the remote default group for IPv4 multicast transmission in each VPN instance on PE 4.

```
[PE4] display multicast-vpn default-group remote
MVPN remote default-group information:
 Group address   Source address  Next hop         VPN instance
```

```
232.1.1.1       1.1.1.1         3.3.3.3         a
232.3.3.3       1.1.1.1         3.3.3.3         b
```

Example: Configuring MDT-based MVPN inter-AS option C

Network configuration

As shown in Figure 14, configure MDT-based MVPN inter-AS option C to meet the following requirements:

Item	Network configuration
Multicast sources and receivers	• In VPN instance **a**, S 1 is a multicast source, and R 2 is a receiver. • In VPN instance **b**, S 2 is a multicast source, and R 1 is a receiver. • For VPN instance **a**, the default group is 239.1.1.1, and the data group range is 225.1.1.0 to 225.1.1.15. • For VPN instance **b**, the default group is 239.4.4.4, and the data group range is 225.4.4.0 to 225.4.4.15.
VPN instances to which PEs belong	• PE 1: VLAN-interface 11 belongs to VPN instance **b**. VLAN-interface 12 belongs to VPN instance **a**. VLAN-interface 2 and Loopback 1 belong to the public network instance. • PE 2: VLAN-interface 2, VLAN-interface 3, Loopback 1, and Loopback 2 belong to the public network instance. • PE 3: VLAN-interface 3, VLAN-interface 4, Loopback 1, and Loopback 2 belong to the public network instance. • PE 4: VLAN-interface 13 belongs to VPN instance **a**. VLAN-interface 14 belongs to VPN instance **b**. VLAN-interface 4 and Loopback 1 belong to the public network instance.
Unicast routing protocols and MPLS	• Configure OSPF separately in AS 100 and AS 200, and configure OSPF between the PEs and CEs. • Establish BGP peer connections between PE 1, PE 2, PE 3, and PE 4 on their respective Loopback 1. • Configure MPLS separately in AS 100 and AS 200.
IP multicast routing	• Enable IP multicast routing on the public network on PE 1, PE 2, PE 3, and PE 4. • Enable IP multicast routing for VPN instance **a** on PE 1 and PE 4. • Enable IP multicast routing for VPN instance **b** on PE 1 and PE 4. • Enable IP multicast routing on CE a1, CE a2, CE b1, and CE b2.
IGMPv2	• Enable IGMPv2 on VLAN-interface 30 of CE a2. • Enable IGMPv2 on VLAN-interface 40 of CE b2.
PIM-SM	Enable PIM-SM on the public network and for VPN instances **a** and **b**: • Enable PIM-SM on all public network interfaces of PE 2 and PE 3. • Enable PIM-SM on all public and private network interfaces of PE 1 and PE 4. • Enable PIM-SM on all interfaces that do not have attached receiver hosts of CE a1, CE a2, CE b1, and CE b2. • Configure Loopback 2 of PE 2 and PE 3 as a C-BSR and a C-RP for their own AS to provide services for all multicast groups. • Configure Loopback 0 of CE a1 as a C-BSR and a C-RP for VPN instance **a** to provide services for all multicast groups. • Configure Loopback 0 of CE b1 as a C-BSR and a C-RP for VPN instance **b** to provide services for all multicast groups.
MSDP	Establish an MSDP peering relationship between PE 2 and PE 3 on their Loopback 1.

Figure 14 Network diagram

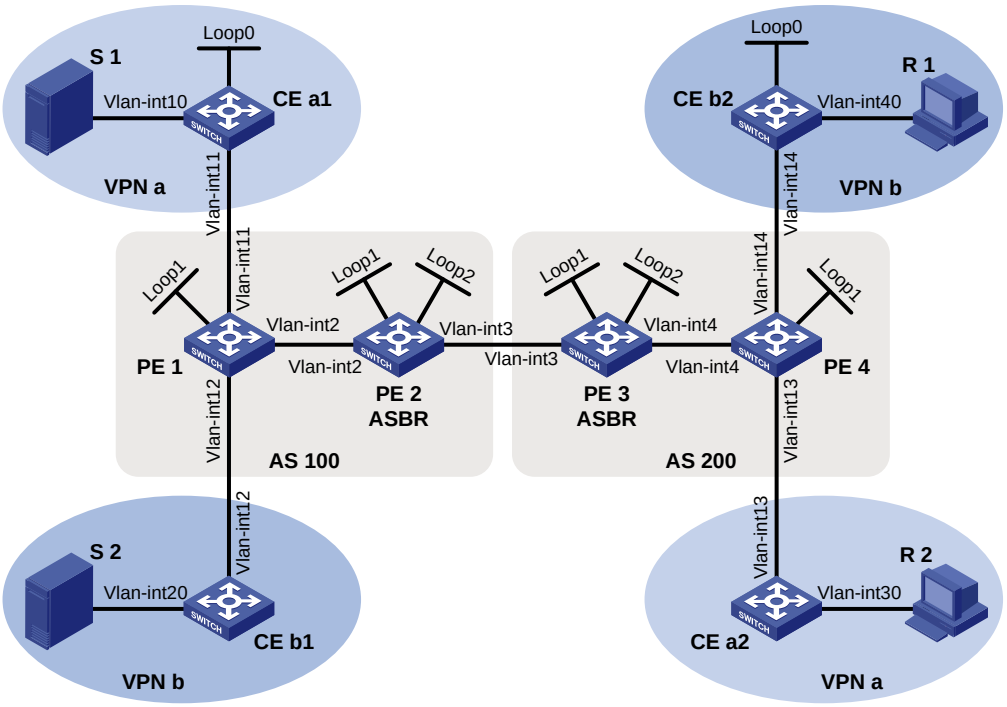


Table 6 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
S 1	—	10.11.5.2/24	R 1	—	10.11.8.2/24
S 2	—	10.11.6.2/24	R 2	—	10.11.7.2/24
PE 1	Vlan-int2	10.10.1.1/24	PE 3	Vlan-int4	10.10.2.1/24
PE 1	Vlan-int11	10.11.1.1/24	PE 3	Vlan-int3	192.168.1.2/24
PE 1	Vlan-int12	10.11.2.1/24	PE 3	Loop1	1.1.1.3/32
PE 1	Loop1	1.1.1.1/32	PE 3	Loop2	22.22.22.22/32
PE 2	Vlan-int2	10.10.1.2/24	PE 4	Vlan-int4	10.10.2.2/24
PE 2	Vlan-int3	192.168.1.1/24	PE 4	Vlan-int13	10.11.3.1/24
PE 2	Loop1	1.1.1.2/32	PE 4	Vlan-int14	10.11.4.1/32
PE 2	Loop2	11.11.11.11/32	PE 4	Loop1	1.1.1.4/32
CE a1	Vlan-int10	10.11.5.1/24	CE b1	Vlan-int20	10.11.6.1/24
CE a1	Vlan-int11	10.11.1.2/24	CE b1	Vlan-int12	10.11.2.2/24
CE a1	Loop0	2.2.2.2/32	CE b2	Vlan-int40	10.11.8.1/24
CE a2	Vlan-int30	10.11.7.1/24	CE b2	Vlan-int14	10.11.4.2/24
CE a2	Vlan-int13	10.11.3.2/24	CE b2	Loop0	3.3.3.3/32

Procedure

1. Configure PE 1:

   # Configure a global router ID, and enable IP multicast routing on the public network.

   ```
   <PE1> system-view
   ```

```
[PE1] router id 1.1.1.1
[PE1] multicast routing
[PE1-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE1] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 2, VLAN 11, or VLAN 12.

```
[PE1] interface gigabitethernet 1/0/4
[PE1-GigabitEthernet1/0/4] port service-loopback group 1
[PE1-GigabitEthernet1/0/4] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-ldp] quit
```

Create a VPN instance named **a**, and configure an RD and route targets for the VPN instance.

```
[PE1] ip vpn-instance a
[PE1-vpn-instance-a] route-distinguisher 100:1
[PE1-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE1-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE1-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE1] multicast routing vpn-instance a
[PE1-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE1] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 address family for VPN instance **a**.

```
[PE1-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE1-mvpn-a-ipv4] default-group 239.1.1.1
[PE1-mvpn-a-ipv4] source loopback 1
[PE1-mvpn-a-ipv4] data-group 225.1.1.0 28
[PE1-mvpn-a-ipv4] quit
[PE1-mvpn-a] quit
```

Create a VPN instance named **b**, and configure an RD and route targets for the VPN instance.

```
[PE1] ip vpn-instance b
[PE1-vpn-instance-b] route-distinguisher 200:1
[PE1-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE1-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE1-vpn-instance-b] quit
```

Enable IP multicast routing for VPN instance **b**.

```
[PE1] multicast routing vpn-instance b
[PE1-mrib-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE1] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv4 address family for VPN instance **b**.

```
[PE1-mvpn-b] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE1-mvpn-b-ipv4] default-group 239.4.4.4
[PE1-mvpn-b-ipv4] source loopback 1
[PE1-mvpn-b-ivp4] data-group 225.4.4.0 28
[PE1-mvpn-b-ipv4] quit
[PE1-mvpn-b] quit
```

Assign an IP address to VLAN-interface 2.

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.10.1.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 2.

```
[PE1-Vlan-interface2] pim sm
[PE1-Vlan-interface2] mpls enable
[PE1-Vlan-interface2] mpls ldp enable
[PE1-Vlan-interface2] quit
```

Associate VLAN-interface 11 with VPN instance **a**.

```
[PE1] interface vlan-interface 11
[PE1-Vlan-interface11] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 11, and enable PIM-SM on the interface.

```
[PE1-Vlan-interface11] ip address 10.11.1.1 24
[PE1-Vlan-interface11] pim sm
[PE1-Vlan-interface11] quit
```

Associate VLAN-interface 12 with VPN instance **b**.

```
[PE1] interface vlan-interface 12
[PE1-Vlan-interface12] ip binding vpn-instance b
```

Assign an IP address to VLAN-interface 12, and enable PIM-SM on the interface.

```
[PE1-Vlan-interface12] ip address 10.11.2.1 24
[PE1-Vlan-interface12] pim sm
[PE1-Vlan-interface12] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] pim sm
[PE1-LoopBack1] quit
```

Configure BGP.

```
[PE1] bgp 100
[PE1-bgp-default] group pe1-pe2 internal
[PE1-bgp-default] peer pe1-pe2 connect-interface loopback 1
[PE1-bgp-default] peer 1.1.1.2 group pe1-pe2
[PE1-bgp-default] group pe1-pe4 external
[PE1-bgp-default] peer pe1-pe4 as-number 200
[PE1-bgp-default] peer pe1-pe4 ebgp-max-hop 255
[PE1-bgp-default] peer pe1-pe4 connect-interface loopback 1
[PE1-bgp-default] peer 1.1.1.4 group pe1-pe4
[PE1–bgp-default] ip vpn-instance a
[PE1-bgp-default-a] address-family ipv4
[PE1-bgp-default-ipv4-a] import-route ospf 2
[PE1-bgp-default-ipv4-a] import-route direct
```

```
[PE1-bgp-default-ipv4-a] quit
[PE1-bgp-default-a] quit
[PE1–bgp-default] ip vpn-instance b
[PE1-bgp-default-b] address-family ipv4
[PE1-bgp-default-ipv4-b] import-route ospf 3
[PE1-bgp-default-ipv4-b] import-route direct
[PE1-bgp-default-ipv4-b] quit
[PE1-bgp-default-b] quit
[PE1–bgp-default] address-family ipv4
[PE1-bgp-default-ipv4] peer pe1-pe2 enable
[PE1-bgp-default-ipv4] peer pe1-pe2 label-route-capability
[PE1-bgp-default-ipv4] quit
[PE1–bgp-default] address-family vpnv4
[PE1–bgp-default-vpnv4] peer pe1-pe4 enable
[PE1–bgp-default-vpnv4] quit
[PE1–bgp-default] quit
```

Configure OSPF.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
[PE1] ospf 2 vpn-instance a
[PE1-ospf-2] import-route bgp
[PE1-ospf-2] area 0.0.0.0
[PE1-ospf-2-area-0.0.0.0] network 10.11.1.0 0.0.0.255
[PE1-ospf-2-area-0.0.0.0] quit
[PE1-ospf-2] quit
[PE1] ospf 3 vpn-instance b
[PE1-ospf-3] import-route bgp
[PE1-ospf-3] area 0.0.0.0
[PE1-ospf-3-area-0.0.0.0] network 10.11.2.0 0.0.0.255
[PE1-ospf-3-area-0.0.0.0] quit
[PE1-ospf-3] quit
```

2. Configure PE 2:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE2> system-view
[PE2] router id 1.1.1.2
[PE2] multicast routing
[PE2-mrib] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE2] mpls lsr-id 1.1.1.2
[PE2] mpls ldp
[PE2-ldp] quit
```

Assign an IP address to VLAN-interface 2.

```
[PE2] interface vlan-interface 2
[PE2-Vlan-interface2] ip address 10.10.1.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 2.

```
[PE2-Vlan-interface2] pim sm
[PE2-Vlan-interface2] mpls enable
[PE2-Vlan-interface2] mpls ldp enable
[PE2-Vlan-interface2] quit
```

Assign an IP address to VLAN-interface 3.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip address 192.168.1.1 24
```

Enable PIM-SM and MPLS on VLAN-interface 3.

```
[PE2-Vlan-interface3] pim sm
[PE2-Vlan-interface3] mpls enable
[PE2-Vlan-interface3] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 1.1.1.2 32
[PE2-LoopBack1] pim sm
[PE2-LoopBack1] quit
```

Assign an IP address to Loopback 2, and enable PIM-SM on the interface.

```
[PE2] interface loopback 2
[PE2-LoopBack2] ip address 11.11.11.11 32
[PE2-LoopBack2] pim sm
[PE2-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[PE2] pim
[PE2-pim] c-bsr 11.11.11.11
[PE2-pim] c-rp 11.11.11.11
[PE2-pim] quit
```

Configure VLAN-interface 3 as a PIM-SM domain border.

```
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] pim bsr-boundary
[PE2-Vlan-interface3] quit
```

Establish an MSDP peering relationship.

```
[PE2] msdp
[PE2-msdp] encap-data-enable
[PE2-msdp] peer 1.1.1.3 connect-interface loopback 1
```

Configure a static route.

```
[PE2] ip route-static 1.1.1.3 32 vlan-interface 3 192.168.1.2
```

Configure BGP.

```
[PE2] bgp 100
[PE2-bgp-default] group pe2-pe1 internal
[PE2-bgp-default] peer pe2-pe1 connect-interface loopback 1
[PE2-bgp-default] peer 1.1.1.1 group pe2-pe1
[PE2-bgp-default] group pe2-pe3 external
[PE2-bgp-default] peer pe2-pe3 as-number 200
[PE2-bgp-default] peer 192.168.1.2 group pe2-pe3
[PE2-bgp-default] address-family ipv4
[PE2-bgp-default-ipv4] peer pe2-pe1 enable
[PE2-bgp-default-ipv4] peer pe2-pe1 route-policy map2 export
```

```
[PE2-bgp-default-ipv4] peer pe2-pe1 label-route-capability
[PE2-bgp-default-ipv4] peer pe2-pe3 enable
[PE2-bgp-default-ipv4] peer pe2-pe3 route-policy map1 export
[PE2-bgp-default-ipv4] peer pe2-pe3 label-route-capability
[PE2-bgp-default-ipv4] import-route ospf 1
[PE2-bgp-default-ipv4] quit
[PE2–bgp-default] quit
```

Configure OSPF.

```
[PE2] ospf 1
[PE2-ospf-1] area 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 1.1.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 11.11.11.11 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.10.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

3. Configure PE 3:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE3> system-view
[PE3] router id 1.1.1.3
[PE3] multicast routing
[PE3-mrib] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE3] mpls lsr-id 1.1.1.3
[PE3] mpls ldp
[PE3-ldp] quit
```

Assign an IP address to VLAN-interface 4.

```
[PE3] interface vlan-interface 4
[PE3-Vlan-interface4] ip address 10.10.2.1 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 4.

```
[PE3-Vlan-interface4] pim sm
[PE3-Vlan-interface4] mpls enable
[PE3-Vlan-interface4] mpls ldp enable
[PE3-Vlan-interface4] quit
```

Assign an IP address to VLAN-interface 3.

```
[PE3] interface vlan-interface 3
[PE3-Vlan-interface3] ip address 192.168.1.2 24
```

Enable PIM-SM and MPLS on VLAN-interface 3.

```
[PE3-Vlan-interface3] pim sm
[PE3-Vlan-interface3] mpls enable
[PE3-Vlan-interface3] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 1.1.1.3 32
[PE3-LoopBack1] pim sm
[PE3-LoopBack1] quit
```

Assign an IP address to Loopback 2, and enable PIM-SM on the interface.

```
[PE3] interface loopback 2
```

```
[PE3-LoopBack2] ip address 22.22.22.22 32
[PE3-LoopBack2] pim sm
[PE3-LoopBack2] quit
```

Configure Loopback 2 as a C-BSR and a C-RP.

```
[PE3] pim
[PE3-pim] c-bsr 22.22.22.22
[PE3-pim] c-rp 22.22.22.22
[PE3-pim] quit
```

Configure VLAN-interface 3 as a PIM-SM domain border.

```
[PE3] interface vlan-interface 3
[PE3-Vlan-interface3] pim bsr-boundary
[PE3-Vlan-interface3] quit
```

Establish an MSDP peering relationship.

```
[PE3] msdp
[PE3-msdp] encap-data-enable
[PE3-msdp] peer 1.1.1.2 connect-interface loopback 1
```

Configure a static route.

```
[PE3] ip route-static 1.1.1.2 32 vlan-interface 3 192.168.1.1
```

Configure BGP.

```
[PE3] bgp 200
[PE3-bgp-default] group pe3-pe4 internal
[PE3-bgp-default] peer pe3-pe4 connect-interface loopback 1
[PE3-bgp-default] peer 1.1.1.4 group pe3-pe4
[PE3-bgp-default] group pe3-pe2 external
[PE3-bgp-default] peer pe3-pe2 as-number 100
[PE3-bgp-default] peer 192.168.1.1 group pe3-pe2
[PE3-bgp-default] address-family ipv4
[PE3-bgp-default-ipv4] peer pe3-pe4 enable
[PE3-bgp-default-ipv4] peer pe3-pe4 route-policy map2 export
[PE3-bgp-default-ipv4] peer pe3-pe4 label-route-capability
[PE3-bgp-default-ipv4] peer pe3-pe2 enable
[PE3-bgp-default-ipv4] peer pe3-pe2 route-policy map1 export
[PE3-bgp-default-ipv4] peer pe3-pe2 label-route-capability
[PE3-bgp-default-ipv4] import-route ospf 1
[PE3-bgp-default-ipv4] quit
[PE3–bgp-default] quit
```

Configure OSPF.

```
[PE3] ospf 1
[PE3-ospf-1] area 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 1.1.1.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 22.22.22.22 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] network 10.10.2.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

4. Configure PE 4:

Configure a global router ID, and enable IP multicast routing on the public network.

```
<PE4> system-view
[PE4] router id 1.1.1.4
```

```
[PE4] multicast routing
[PE4-mrib] quit
```

Create service loopback group 1, and specify the multicast tunnel service for the group.

```
[PE4] service-loopback group 1 type multicast-tunnel
```

Assign GigabitEthernet 1/0/4 to service loopback group 1. The interface does not belong to VLAN 4, VLAN 13, or VLAN 14.

```
[PE4] interface gigabitethernet 1/0/4
[PE4-GigabitEthernet1/0/4] port service-loopback group 1
[PE4-] quit
```

Configure an LSR ID, and enable LDP globally.

```
[PE4] mpls lsr-id 1.1.1.4
[PE4] mpls ldp
[PE4-ldp] quit
```

Create a VPN instance named **a**, and configure an RD and route targets for the VPN instance.

```
[PE4] ip vpn-instance a
[PE4-vpn-instance-a] route-distinguisher 100:1
[PE4-vpn-instance-a] vpn-target 100:1 export-extcommunity
[PE4-vpn-instance-a] vpn-target 100:1 import-extcommunity
[PE4-vpn-instance-a] quit
```

Enable IP multicast routing for VPN instance **a**.

```
[PE4] multicast routing vpn-instance a
[PE4-mrib-a] quit
```

Create an MDT-based MVPN for VPN instance **a**.

```
[PE4] multicast-vpn vpn-instance a mode mdt
```

Create an MVPN IPv4 address family for VPN instance **a**.

```
[PE4-mvpn-a] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **a**.

```
[PE4-mvpn-a-ipv4] default-group 239.1.1.1
[PE4-mvpn-a-ivp4] source loopback 1
[PE4-mvpn-a-ivp4] data-group 225.1.1.0 28
[PE4-mvpn-a-ipv4] quit
[PE4-mvpn-a] quit
```

Create a VPN instance named **b**, and configure an RD and route targets for the VPN instance.

```
[PE4] ip vpn-instance b
[PE4-vpn-instance-b] route-distinguisher 200:1
[PE4-vpn-instance-b] vpn-target 200:1 export-extcommunity
[PE4-vpn-instance-b] vpn-target 200:1 import-extcommunity
[PE4-vpn-instance-b] quit
```

Enable IP multicast routing for VPN instance **b**.

```
[PE4] multicast routing vpn-instance b
[PE4-mrib-b] quit
```

Create an MDT-based MVPN for VPN instance **b**.

```
[PE4] multicast-vpn vpn-instance b mode mdt
```

Create an MVPN IPv4 address family for VPN instance **b**.

```
[PE4-mvpn-b] address-family ipv4
```

Specify the default group, the MVPN source interface, and the data group range for VPN instance **b**.

```
[PE4-mvpn-b-ipv4] default-group 239.4.4.4
[PE4-mvpn-b-ipv4] source loopback 1
[PE4-mvpn-b-ivp4] data-group 225.4.4.0 28
[PE4-mvpn-b-ipv4] quit
[PE4-mvpn-b] quit
```

Assign an IP address to VLAN-interface 4.

```
[PE4] interface vlan-interface 4
[PE4-Vlan-interface4] ip address 10.10.2.2 24
```

Enable PIM-SM, MPLS, and IPv4 LDP on VLAN-interface 4.

```
[PE4-Vlan-interface4] pim sm
[PE4-Vlan-interface4] mpls enable
[PE4-Vlan-interface4] mpls ldp enable
[PE4-Vlan-interface4] quit
```

Associate VLAN-interface 13 with VPN instance **a**.

```
[PE4] interface vlan-interface 13
[PE4-Vlan-interface13] ip binding vpn-instance a
```

Assign an IP address to VLAN-interface 13, and enable PIM-SM on the interface.

```
[PE4-Vlan-interface13] ip address 10.11.3.1 24
[PE4-Vlan-interface13] pim sm
[PE4-Vlan-interface13] quit
```

Associate VLAN-interface 14 with VPN instance **b**.

```
[PE4] interface vlan-interface 14
[PE4-Vlan-interface14] ip binding vpn-instance b
```

Assign an IP address to VLAN-interface 14, and enable PIM-SM on the interface.

```
[PE4-Vlan-interface14] ip address 10.11.4.1 24
[PE4-Vlan-interface14] pim sm
[PE4-Vlan-interface14] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[PE4] interface loopback 1
[PE4-LoopBack1] ip address 1.1.1.4 32
[PE4-LoopBack1] pim sm
[PE4-LoopBack1] quit
```

Configure BGP.

```
[PE4] bgp 200
[PE4-bgp-default] group pe4-pe3 internal
[PE4-bgp-default] peer pe4-pe3 connect-interface loopback 1
[PE4-bgp-default] peer 1.1.1.3 group pe4-pe3
[PE4-bgp-default] group pe4-pe1 external
[PE4-bgp-default] peer pe4-pe1 as-number 100
[PE4-bgp-default] peer pe4-pe1 ebgp-max-hop 255
[PE4-bgp-default] peer pe4-pe1 connect-interface loopback 1
[PE4-bgp-default] peer 1.1.1.1 group pe4-pe1
[PE4–bgp-default] ip vpn-instance a
[PE4-bgp-default-a] address-family ipv4
[PE4-bgp-default-ipv4-a] import-route ospf 2
[PE4-bgp-default-ipv4-a] import-route direct
[PE4-bgp-default-ipv4-a] quit
[PE4-bgp-default-a] quit
```

```
[PE4–bgp-default] ip vpn-instance b
[PE4-bgp-default-b] address-family ipv4
[PE4-bgp-default-ipv4-b] import-route ospf 3
[PE4-bgp-default-ipv4-b] import-route direct
[PE4-bgp-default-ipv4-b] quit
[PE4-bgp-default-b] quit
[PE4–bgp-default] address-family ipv4
[PE4-bgp-default-ipv4] peer pe4-pe3 enable
[PE4-bgp-default-ipv4] peer pe4-pe3 label-route-capability
[PE4-bgp-default-ipv4] quit
[PE4–bgp-default] address-family vpnv4
[PE4–bgp-default-vpnv4] peer pe4-pe1 enable
[PE4–bgp-default-vpnv4] quit
[PE4–bgp-default] quit
```

Configure OSPF.

```
[PE4] ospf 1
[PE4-ospf-1] area 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 1.1.1.4 0.0.0.0
[PE4-ospf-1-area-0.0.0.0] network 10.10.2.0 0.0.0.255
[PE4-ospf-1-area-0.0.0.0] quit
[PE4-ospf-1] quit
[PE4] ospf 2 vpn-instance a
[PE4-ospf-2] import-route bgp
[PE4-ospf-2] area 0.0.0.0
[PE4-ospf-2-area-0.0.0.0] network 10.11.3.0 0.0.0.255
[PE4-ospf-2-area-0.0.0.0] quit
[PE4-ospf-2] quit
[PE4] ospf 3 vpn-instance b
[PE4-ospf-3] import-route bgp
[PE4-ospf-3] area 0.0.0.0
[PE4-ospf-3-area-0.0.0.0] network 10.11.4.0 0.0.0.255
[PE4-ospf-3-area-0.0.0.0] quit
[PE4-ospf-3] quit
```

5. Configure CE a1:

Enable IP multicast routing.

```
<CEa1> system-view
[CEa1] multicast routing
[CEa1-mrib] quit
```

Assign an IP address to VLAN-interface 10, and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 10
[CEa1-Vlan-interface10] ip address 10.11.5.1 24
[CEa1-Vlan-interface10] pim sm
[CEa1-Vlan-interface10] quit
```

Assign an IP address to VLAN-interface 11, and enable PIM-SM on the interface.

```
[CEa1] interface vlan-interface 11
[CEa1-Vlan-interface11] ip address 10.11.1.2 24
[CEa1-Vlan-interface11] pim sm
[CEa1-Vlan-interface11] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[CEa1] interface loopback 1
[CEa1-LoopBack1] ip address 2.2.2.2 32
[CEa1-LoopBack1] pim sm
[CEa1-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[CEa1] pim
[CEa1-pim] c-bsr 2.2.2.2
[CEa1-pim] c-rp 2.2.2.2
[CEa1-pim] quit
```

Configure OSPF.

```
[CEa1] ospf 1
[CEa1-ospf-1] area 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[CEa1-ospf-1-area-0.0.0.0] network 10.11.1.0 0.0.0.255
[CEa1-ospf-1-area-0.0.0.0] network 10.11.5.0 0.0.0.255
[CEa1-ospf-1-area-0.0.0.0] quit
[CEa1-ospf-1] quit
```

6. Configure CE b1:

Enable IP multicast routing.

```
<CEb1> system-view
[CEb1] multicast routing
[CEb1-mrib] quit
```

Assign an IP address to VLAN-interface 20, and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 20
[CEb1-Vlan-interface20] ip address 10.11.6.1 24
[CEb1-Vlan-interface20] pim sm
[CEb1-Vlan-interface20] quit
```

Assign an IP address to VLAN-interface 12, and enable PIM-SM on the interface.

```
[CEb1] interface vlan-interface 12
[CEb1-Vlan-interface12] ip address 10.11.2.2 24
[CEb1-Vlan-interface12] pim sm
[CEb1-Vlan-interface12] quit
```

Configure OSPF.

```
[CEb1] ospf 1
[CEb1-ospf-1] area 0.0.0.0
[CEb1-ospf-1-area-0.0.0.0] network 10.11.2.0 0.0.0.255
[CEb1-ospf-1-area-0.0.0.0] network 10.11.6.0 0.0.0.255
[CEb1-ospf-1-area-0.0.0.0] quit
[CEb1-ospf-1] quit
```

7. Configure CE a2:

Enable IP multicast routing.

```
<CEa2> system-view
[CEa2] multicast routing
[CEa2-mrib] quit
```

Assign an IP address to VLAN-interface 30, and enable IGMP on the interface.

```
[CEa2] interface vlan-interface 30
```

```
[CEa2-Vlan-interface30] ip address 10.11.7.1 24
[CEa2-Vlan-interface30] igmp enable
[CEa2-Vlan-interface30] quit
```

Assign an IP address to VLAN-interface 13, and enable PIM-SM on the interface.

```
[CEa2] interface vlan-interface 13
[CEa2-Vlan-interface13] ip address 10.11.3.2 24
[CEa2-Vlan-interface13] pim sm
[CEa2-Vlan-interface13] quit
```

Configure OSPF.

```
[CEa2] ospf 1
[CEa2-ospf-1] area 0.0.0.0
[CEa2-ospf-1-area-0.0.0.0] network 10.11.3.0 0.0.0.255
[CEa2-ospf-1-area-0.0.0.0] network 10.11.7.0 0.0.0.255
[CEa2-ospf-1-area-0.0.0.0] quit
[CEa2-ospf-1] quit
```

8. Configure CE b2:

Enable IP multicast routing.

```
<CEb2> system-view
[CEb2] multicast routing
[CEb2-mrib] quit
```

Assign an IP address to VLAN-interface 40, and enable IGMP on the interface.

```
[CEb2] interface vlan-interface 40
[CEb2-Vlan-interface40] ip address 10.11.8.1 24
[CEb2-Vlan-interface40] igmp enable
[CEb2-Vlan-interface40] quit
```

Assign an IP address to VLAN-interface 14, and enable PIM-SM on the interface.

```
[CEb2] interface vlan-interface 14
[CEb2-Vlan-interface14] ip address 10.11.4.2 24
[CEb2-Vlan-interface14] pim sm
[CEb2-Vlan-interface14] quit
```

Assign an IP address to Loopback 1, and enable PIM-SM on the interface.

```
[CEb2] interface loopback 1
[CEb2-LoopBack1] ip address 3.3.3.3 32
[CEb2-LoopBack1] pim sm
[CEb2-LoopBack1] quit
```

Configure Loopback 1 as a C-BSR and a C-RP.

```
[CEb2] pim
[CEb2-pim] c-bsr 3.3.3.3
[CEb2-pim] c-rp 3.3.3.3
[CEb2-pim] quit
```

Configure OSPF.

```
[CEb2] ospf 1
[CEb2-ospf-1] area 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[CEb2-ospf-1-area-0.0.0.0] network 10.11.4.0 0.0.0.255
[CEb2-ospf-1-area-0.0.0.0] network 10.11.8.0 0.0.0.255
[CEb2-ospf-1-area-0.0.0.0] quit
```

```
[CEb2-ospf-1] quit
```

Verifying the configuration

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 1.

```
[PE1] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      a
 239.4.4.4        1.1.1.1          MTunnel1      b
```

Display information about the local default group for IPv4 multicast transmission in each VPN instance on PE 4.

```
[PE4] display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.4          MTunnel0      a
 239.4.4.4        1.1.1.4          MTunnel1      b
```

Troubleshooting MDT-based MVPN

This section describes common MDT-based MVPN problems and how to troubleshoot them.

A default MDT cannot be established

Symptom

The default MDT cannot be established. PIM neighboring relationship cannot be established between PEs' interfaces that are in the same VPN instance.

Solution

To resolve the problem:

1. Use the **display interface** command to examine the MTI interface state and address encapsulation on the MTI.
2. Use the **display multicast-vpn default-group** command to verify that the same default group address has been configured for the same VPN instance on different PEs.
3. Use the **display pim interface** command to verify the following:
   - PIM is enabled on a minimum of one interface of the same VPN on different PEs.
   - The same PIM mode is running on all the interfaces of the same VPN instance on different PEs and on all the interfaces of the P device.
4. Use the **display ip routing-table** command to verify that a unicast route exists from the VPN instance on the local PE to the same VPN instance on each remote PE.
5. Use the **display bgp peer** command to verify that the BGP peer connections have been correctly configured.
6. If the problem persists, contact Hewlett Packard Enterprise Support.

An MVRF cannot be created

Symptom

A VPN instance cannot create an MVRF correctly.

Solution

To resolve the problem:

1. Use the **display pim bsr-info** command to verify that the BSR information exists on the public network and VPN instance. If it does not, verify that a unicast route exists to the BSR.
2. Use the **display pim rp-info** command to examine the RP information. If no RP information is available, verify that a unicast route exists to the RP. Use the **display pim neighbor** command to verify that the PIM adjacencies have been correctly established on the public network and the VPN.
3. Use the **ping** command to examine the connectivity between the VPN DR and the VPN RP.
4. If the problem persists, contact Hewlett Packard Enterprise Support.

Command reference

address-family ipv4

Use **address-family ipv4** to create an MVPN IPv4 address family and enter its view, or enter the view of the existing MVPN IPv4 address family.

Use **undo address-family ipv4** to delete the MVPN IPv4 address family and configurations in MVPN IPv4 address family view.

Syntax

address-family ipv4

undo address-family ipv4

Default

No MVPN IPv4 address family exists.

Views

MVPN view

Predefined user roles

network-admin

Usage guidelines

Configurations in MVPN IPv4 address family view of a VPN instance apply only to IPv4 multicast packets of that instance.

Examples

In MVPN view of VPN instance **mvpn**, create an MVPN IPv4 address family and enter its view.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv4
[Sysname-mvpn-mvpn-ipv4]
```

address-family ipv4 mdt

Use **address-family ipv4 mdt** to create a BGP IPv4 MDT address family and enter its view, or enter the view of the existing BGP IPv4 MDT address family.

Use **undo address-family ipv4 mdt** to delete the BGP IPv4 MDT address family and all configurations in BGP IPv4 MDT address family view.

Syntax

address-family ipv4 mdt

undo address-family ipv4 mdt

Default

No BGP IPv4 MDT address family exists.

Views

BGP instance view

Predefined user roles

network-admin

Usage guidelines

Execute this command before you use the **peer enable** command to enable BGP peers to exchange MDT information. MDT information includes the IP address of a PE device and the default group to which the PE device belongs. On a public network running PIM-SSM, multicast VPN establishes a default MDT rooted at the PE device (multicast source) based on the MDT information.

Configurations in BGP IPv4 MDT address family view take effect only on BGP MDT messages, BGP MDT peers, and BGP MDT peer groups.

Examples

In BGP instance view of BGP instance **default**, create a BGP IPv4 MDT address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] address-family ipv4 mdt
[Sysname-bgp-default-mdt]
```

In BGP instance view of BGP instance **abc**, create a BGP IPv4 MDT address family and enter its view.

```
<Sysname> system-view
[Sysname] bgp 100 instance abc
[Sysname-bgp-abc] address-family ipv4 mdt
[Sysname-bgp-abc-mdt]
```

Related commands

peer enable (see *Layer 3—IP Routing Command Reference*)

address-family ipv6

Use **address-family ipv6** to create an MVPN IPv6 address family and enter its view, or enter the view of the existing MVPN IPv6 address family.

Use **undo address-family ipv6** to delete the MVPN IPv6 address family and configurations in MVPN IPv6 address family view.

Syntax

address-family ipv6

undo address-family ipv6

Default

No MVPN IPv6 address family exists.

Views

MVPN view

Predefined user roles

network-admin

Usage guidelines

Configurations in MVPN IPv6 address family view of a VPN instance apply only to IPv6 multicast packets of that instance.

Examples

In MVPN view of VPN instance **mvpn**, create an MVPN IPv6 address family and enter its view.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv6
[Sysname-mvpn-mvpn-ipv6]
```

data-delay

Use **data-delay** to set the data-delay period (delay period before the device switches over from the default MDT to the data MDT).

Use **undo data-delay** to restore the default.

Syntax

data-delay *delay*

undo data-delay

Default

The data-delay period is 3 seconds.

Views

MVPN IPv4 address family view

MVPN IPv6 address family view

Predefined user roles

network-admin

Parameters

delay: Specifies a data-delay period in the range of 1 to 60 seconds.

Examples

In MVPN IPv4 address family view of VPN instance **mvpn**, set the data-delay period to 20 seconds.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv4
[Sysname-mvpn-mvpn-ipv4] data-delay 20
```

data-group

Use **data-group** to specify a data group range and optionally configure the criteria for the device to initiate a switchover of the default MDT to a data MDT.

Use **undo data-group** to restore the default.

Syntax

data-group *group-address* { *mask-length* | *mask* } [**acl** *acl-number*]

undo data-group

Default

No data group range exists, and the device never initiates a switchover of the default MDT to a data MDT.

Views

MVPN IPv4 address family view

MVPN IPv6 address family view

Predefined user roles

network-admin

Parameters

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

mask-length: Specifies a mask length for the multicast group address, in the range of 25 to 32.

mask: Specifies a subnet mask for the multicast group address.

acl *acl-number*: Specifies an advanced ACL by its number in the range of 3000 to 3999. If you specify an ACL, the multicast data permitted by the ACL can trigger the switchover. If you do not specify an ACL, any multicast data can trigger the switchover. For the ACL to take effect, specify the protocol type as IP, and include the **source** and **destination** keywords when you create an ACL rule. The **source** and **destination** keywords specify a multicast source address range and a multicast group address range, respectively.

Usage guidelines

On a PE, the data group range for an MVPN cannot include the default group or data groups of any other MVPN. For an MVPN that transmits both IPv4 and IPv6 multicast packets, the data group ranges in MVPN IPv4 address family view and MVPN IPv6 address family view cannot overlap.

All VPN instances share the data group resources. As a best practice to avoid data group resource exhaustion, specify a reasonable data group range for a VPN instance.

The data group ranges for different MDs on different PE devices cannot overlap with one another if the PIM mode is not PIM-SSM on the public network.

If you execute this command multiple times in the same MVPN IPv4 address family view or IPv6 address family view, the most recent configuration takes effect.

Examples

In MVPN IPv4 address family view of VPN instance **mvpn**, specify 239.1.2.192 through 239.1.2.255 as the data group range.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv4
[Sysname-mvpn-mvpn-ipv4] data-group 239.1.2.192.25
```

default-group

Use **default-group** to specify a default group.

Use **undo default-group** to restore the default.

Syntax

default-group *group-address*

undo default-group

Default

No default group exists.

Views

MVPN IPv4 address family view

MVPN IPv6 address family view

Predefined user roles

network-admin

Parameters

group-address: Specifies a default group in the range of 224.0.1.0 to 239.255.255.255.

Usage guidelines

You must specify the same default group on all PE devices that belong to the same MVPN.

The default group for an MVPN must be different from the default group and the data group used by any other MVPN.

For an MVPN that transmits both IPv4 and IPv6 multicast packets, you must specify the same default group in MVPN IPv4 address family view and MVPN IPv6 address family view.

Examples

In MVPN IPv4 address family view and IPv6 address family view of VPN instance **mvpn**, specify 239.1.1.1 as the default group.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv4
[Sysname-mvpn-mvpn-ipv4] default-group 239.1.1.1
[Sysname-mvpn-mvpn-ipv4] quit
[Sysname-mvpn-mvpn] address-family ipv6
[Sysname-mvpn-mvpn-ipv6] default-group 239.1.1.1
```

display bgp routing-table ipv4 mdt

Use **display bgp routing-table ipv4 mdt** to display BGP MDT routing information.

Syntax

display bgp [**instance** *instance-name*] **routing-table ipv4 mdt** [**route-distinguisher** *route-distinguisher*] [*ip-address* [**advertise-info**]]

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 MDT routing information for BGP instance **default**.

route-distinguisher *route-distinguisher*: Specifies an RD, a string of 3 to 21 characters. If you do not specify an RD, this command displays BGP MDT routing information for all RDs. An RD can be 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, where the AS number must be equal to or greater than 65536. For example, 65536:1.

ip-address: Specifies a multicast source by its IP address. The *ip-address* argument represents the IP address of the PE device in the default MDT. If you do not specify a multicast source, this command displays brief information about BGP MDT routes for all multicast sources.

advertise-info: Displays advertisement information. If you do not specify this keyword, no advertisement information is displayed.

Examples

Display brief information about BGP MDT routes for all multicast sources.

```
<Sysname> display bgp routing-table ipv4 mdt

 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
               Origin: i - IGP, e - EGP, ? - incomplete

 Route distinguisher: 100:1
 Total number of routes: 2

     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

* >  1.1.1.1/32         0.0.0.0                               32768   ?
* >i 2.2.2.2/32         2.2.2.2                   100         0       ?
```

Display detailed information about BGP MDT routes for multicast source 1.1.1.1.

```
<Sysname> display bgp routing-table ipv4 mdt 1.1.1.1

 BGP local router ID: 1.1.1.1
 Local AS number: 100



 Route distinguisher: 100:1
 Total number of routes: 1
 Paths:   1 available, 1 best

 BGP MDT information of source 1.1.1.1:
 Default-group   : 224.1.1.1
 Original nexthop: 0.0.0.0
 AS-path         : (null)
 Origin          : incomplete
 Attribute value : pref-val 32768
 State           : valid, local, best
IP precedence   : N/A
 QoS local ID    : N/A
```

```
 Traffic index   : N/A
```

Display advertisement information about BGP MDT routes for multicast source 1.1.1.1.

```
<Sysname> display bgp routing-table ipv4 mdt 1.1.1.1 advertise-info

 BGP local router ID: 1.1.1.1
 Local AS number: 100

 Route distinguisher: 100:1
 Total number of routes: 1
 Paths:   1 best

 BGP MDT information of source 1.1.1.1:
 Default-group: 224.1.1.1
 Advertised to peers (1 in total):
     6.6.6.6
```

Table 7 Command output

Field	Description
BGP local router ID	ID of the local router.
Status codes	Codes of route status: • *** – valid**—Valid route. • **> – best**—Optimal route. • **d – damped**—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 information: • **IGP**—Originated in the AS. • **EGP**—Learned through EGP. • **incomplete**—Learned by some other means.
Total number of routes	Total number of BGP MDT routes.
Network	Source IP address of the default MDT.
NextHop	IP address of the next hop.
MED	Attribute value of Multi-Exit-Discrimination (MED).
LocPrf	Local preference value.
PrefVal	Preferred value of a route.
Path/Ogn	AS PATH attribute and ORIGIN attribute: • **AS_PATH**—Records the ASs the packet has passed to avoid routing loops. • **ORIGIN**—Identifies the origin of the BGP MDT routes.
Paths	Number of the BGP MDT routes: • **available**—Number of valid BGP MDT routes. • **best**—Number of the optimal BGP MDT routes.
BGP MDT information of source	BGP MDT routing information for the multicast source 1.1.1.1.

Field	Description
1.1.1.1	
Default-group	Default-group address to which the route belongs.
Advertised to peers (1 in total)	Peers to which the route has been advertised and total number of peers.
From	IP address of the BGP peer that advertises the BGP MDT route.
Original nexthop	IP address of the original next hop. If the BGP MDT route is learned from the BGP update message, this field displays the IP address of the next hop that receives the message.
AS-path	AS PATH attribute of the path, recording the ASs that the BGP MDT route has passed to avoid routing loops.
Attribute value	Attributes of the BGP MDT routes: • **MED**—MED value related to destination network. • **Localpref**—Local preferred value. • **pref-val**—Preferred value of the route. • **pre**—Preferred value of the protocol.
State	Current states: • **valid**—Valid routes. • **internal**—Internal routes. • **external**—External routes. • **local**—Local routes. • **synchronize**—Synchronized routes. • **best**—Optimal routes.
IP precedence	IP precedence of the route, which is set by the QPPB feature. This field displays **N/A** if the route does not carry this attribute.
QoS local ID	QoS local ID of the route, which is set by the QPPB feature. This field displays **N/A** if the route does not carry this attribute.
Traffic index	Traffic index of the route, which is set by the QPPB feature. This field displays **N/A** if the route does not carry this attribute.

display multicast-vpn data-group receive

Use **display multicast-vpn data-group receive** to display information about data groups for IPv4 multicast transmission that are received in a VPN instance.

Syntax

display multicast-vpn vpn-instance *vpn-instance-name* **data-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *]

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.

brief: Displays brief information. If you do not specify this keyword, the command displays detailed information.

active: Specifies data groups that have joined the data MDT.

group *group-address*: Specifies a data group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

sender *source-address*: Specifies an MVPN source interface by its IP address.

vpn-source-address: Specifies a multicast source address of the specified VPN instance.

vpn-group-address: Specifies a multicast group address of the specified VPN instance. The value range for this argument is 224.0.0.0 to 239.255.255.255.

mask-length: Specifies a mask length of the specified multicast source address or multicast group address. The value range for this argument is 0 to 32, and the default is 32.

mask: Specifies a subnet mask of the specified multicast source address or multicast group address. The default is 255.255.255.255.

Examples

Display detailed information about data groups for IPv4 multicast transmission that are received in VPN instance **mvpn**.

```
<Sysname> display multicast-vpn vpn-instance mvpn data-group receive
MVPN data-group information received by VPN instance: mvpn
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched

Data-group: 226.1.1.0   Reference count: 4   Active count: 2
  Sender: 172.100.1.1   Active count: 1
    (192.6.1.5, 239.1.1.1)       expires: 00:03:10 active
    (192.6.1.5, 239.1.1.158)     expires: 00:03:10
  Sender:  181.100.1.1, active count: 1
    (195.6.1.2, 239.1.2.12)      expires: 00:03:10 active
    (195.6.1.2, 239.1.2.197)     expires: 00:03:10
Data-group: 229.1.1.0   Reference count: 4   Active count: 2
  Sender: 185.100.1.1   Active count: 1
    (198.6.1.5, 239.1.3.62)      expires: 00:03:10 active
    (198.6.1.5, 225.1.1.109)     expires: 00:03:10
  Sender: 190.100.1.1   Active count: 1
    (200.6.1.2, 225.1.4.80)      expires: 00:03:10 active
    (200.6.1.2, 225.1.4.173)     expires: 00:03:10
```

Display brief information about data groups for IPv4 multicast transmission that are received in VPN instance **mvpn**.

```
<Sysname> display multicast-vpn vpn-instance mvpn data-group receive brief
MVPN data-group information received by VPN instance: mvpn
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched

Data-group: 226.1.1.0   Reference count: 4   Active count: 2
Data-group: 229.1.1.0   Reference count: 4   Active count: 2
```

Table 8 Command output

Field	Description
MVPN data-group information received by VPN instance: mvpn	Information about data groups for IPv4 multicast transmission that are received in VPN instance **mvpn**.
Total 2 data-groups for 8 entries	A total of 2 data groups, associated with 8 (S, G) entries.
Total 2 data-groups and 8 entries matched	A total of 2 matching data groups, associated with 8 (S, G) entries.
Data-group	IP address of the received data group.
Sender	BGP peer address of the PE device that sent the data group.
Reference count	Number of (S, G) entries that use the data group in the VPN instance.
Active count	Number of active (S, G) entries (entries with active receivers) that use the data group in the VPN instance.
expires	Remaining time for the (S, G) entry that uses the data group in the VPN instance.

display multicast-vpn data-group send

Use **display multicast-vpn data-group send** to display information about data groups for IPv4 multicast transmission that are sent in a VPN instance.

Syntax

display multicast-vpn vpn-instance *vpn-instance-name* **data-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *

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.

group *group-address*: Specifies a data group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

reuse *interval*: Specifies an interval during which data group reuses occur, in the range of 1 to 2147483647 seconds.

vpn-source-address: Specifies a multicast source address of the specified VPN instance.

vpn-group-address: Specifies a multicast group address of the specified VPN instance. The value range for this argument is 224.0.0.0 to 239.255.255.255.

mask-length: Specifies a mask length of the specified multicast source address or multicast group address. The value range for this argument is 0 to 32, and the default is 32.

mask: Specifies a subnet mask of the specified multicast source address or multicast group address. The default is 255.255.255.255.

Examples

Display information about data groups for IPv4 multicast transmission that are sent in VPN instance **mvpn**.

```
<Sysname> display multicast-vpn vpn-instance mvpn data-group send
MVPN data-group information sent by VPN instance: mvpn
Total 2 data-groups for 6 entries
Total 2 data-groups and 6 entries matched

  Reference count of 226.1.1.0: 3
    (192.6.1.5, 239.1.1.1)                 switch time: 00:00:21
    (192.6.1.5, 239.1.1.158)               switch time: 00:00:21
    (192.6.1.5, 239.1.2.50)                switch time: 00:00:05
  Reference count of 226.1.1.1: 3
    (192.6.1.2, 225.1.1.1)                 switch time: 00:00:21
    (192.6.1.2, 225.1.2.50)                switch time: 00:00:05
    (192.6.1.5, 239.1.1.159)               switch time: 00:00:21
```

Display reuse information about data groups for IPv4 multicast transmission that are sent in VPN instance **mvpn** within 30 seconds.

```
<Sysname> display multicast-vpn vpn-instance mvpn data-group send reuse 30
MVPN data-group information sent by VPN instance: mvpn
Total 2 data-groups for 3 entries
Total 2 data-groups and 3 entries matched

  Reuse count of 226.1.1.0: 1
  Reuse count of 226.1.1.1: 1
  Reuse count of 226.1.1.2: 1
```

Table 9 Command output

Field	Description
MVPN data-group information sent by VPN instance: mvpn	Information about data groups for IPv4 multicast transmission that are sent in VPN instance **mvpn**.
Total 2 data-groups for 6 entries	A total of 2 data groups, associated with 6 (S, G) entries.
Total 2 data-groups and 6 entries matched	A total of 2 matching data groups, associated with 6 (S, G) entries.
Reference count of 226.1.1.0	Number of (S, G) entries that use the data group in the VPN instance.
switch time	Switchover time of the (S, G) entry that uses the data group in the VPN instance.
Reuse count of 226.1.1.0	Number of times that the data group is reused during the specified length of time.

display multicast-vpn default-group

Use **display multicast-vpn default-group** to display information about default groups for IPv4 multicast transmission.

Syntax

display multicast-vpn [**vpn-instance** *vpn-instance-name*] **default-group** { **local** | **remote** }

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 information about default groups of all VPN instances for IPv4 multicast transmission.

local: Specifies local default groups for IPv4 multicast transmission.

remote: Specifies remote default groups for IPv4 multicast transmission.

Examples

Display information about the local default group for IPv4 multicast transmission in each VPN instance.

```
<Sysname> display multicast-vpn default-group local
MVPN local default-group information:
 Group address    Source address   Interface     VPN instance
 239.1.1.1        1.1.1.1          MTunnel0      mvpna
 239.2.1.1        1.1.1.1          MTunnel1      mvpnb
 239.3.1.1        --               MTunnel2      mvpnc
```

Display information about the remote default group for IPv4 multicast transmission in each VPN instance.

```
<Sysname> display multicast-vpn default-group remote
MVPN remote default-group information:
 Group address   Source address  Next hop         VPN instance
 239.1.1.1       1.2.0.1         1.2.0.1          a
 239.1.1.1       1.2.0.2         1.2.0.2          a
 239.1.1.1       1.2.0.3         1.2.0.3          a
 239.1.1.2       1.2.0.1         1.2.0.1          b
 239.1.1.2       1.2.0.2         1.2.0.2          b
 239.1.1.3       1.2.0.1         1.2.0.1          -
```

Table 10 Command output

Field	Description
Group address	IP address of the default group for IPv4 multicast transmission.
Source address	IP address of the MVPN source interface, which is used by the MTI as the source address to encapsulate multicast packets for the VPN instance.
Interface	MTI interface.
Next hop	IP address of the next hop.
VPN instance	VPN instance to which the default group belongs.

display multicast-vpn ipv6 data-group receive

Use **display multicast-vpn ipv6 data-group receive** to display information about data groups for IPv6 multicast transmission that are received in a VPN instance.

Syntax

display multicast-vpn vpn-instance *vpn-instance-name* **ipv6 data-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [*mask-length*] | *vpn-group-address* [*mask-length*]] *]

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.

brief: Displays brief information. If you do not specify this keyword, the command displays detailed information.

active: Specifies data groups that have joined the data MDT.

group *group-address*: Specifies a data group by its address in the range of 224.0.1.0 to 239.255.255.255.

sender *source-address*: Specifies an MVPN source interface by its address.

vpn-source-address: Specifies an IPv6 multicast source address of the specified VPN instance.

vpn-group-address: Specifies an IPv6 multicast group address of the specified VPN instance. The value range for this argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F.

mask-length: Specifies a mask length of the specified IPv6 multicast source address or IPv6 multicast group address. For the IPv6 multicast source address, the value range for this argument is 8 to 128, and the default is 128. For the IPv6 multicast group address, the value range for this argument is 0 to 128, and the default is 128.

Examples

Display detailed information about data groups for IPv6 multicast transmission that are received in VPN instance **mvpn**.

```
<Sysname> display multicast-vpn vpn-instance mvpn ipv6 data-group receive
MVPN data-group information received by VPN instance: mvpn
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched

Data-group: 226.1.1.0   Reference count: 4   Active count: 2
Sender: 172.100.1.1   Active count: 1
(192::1, ff1e::1)
expires: 00:03:10 active
(192::1, ff1e::2)
expires: 00:03:10
Sender:  181.100.1.1, active count: 1
(192::2, ff1e::11)
expires: 00:03:10 active
(192::2, ff1e::12)
expires: 00:03:10
Data-group: 229.1.1.0   Reference count: 4   Active count: 2
```

```
Sender: 185.100.1.1   Active count: 1
(192::6, ff1e::15)
expires: 00:03:10 active
(192::6, ff1e::16)
expires: 00:03:10
Sender: 190.100.1.1   Active count: 1
(192::11, ff1e::21)
expires: 00:03:10 active
(192::11, ff1e::22)
expires: 00:03:10
```

Display brief information about data groups for IPv6 multicast transmission that are received in VPN instance **mvpn**.

```
<Sysname> display multicast-vpn vpn-instance mvpn ipv6 data-group receive brief
MVPN data-group information received by VPN instance: mvpn
Total 2 data-groups for 8 entries
Total 2 data-groups and 8 entries matched

Data-group: 226.1.1.0   Reference count: 4   Active count: 2
Data-group: 229.1.1.0   Reference count: 4   Active count: 2
```

Table 11 Command output

Field	Description
MVPN data-group information received by VPN instance: mvpn	Information about data groups for IPv6 multicast transmission that are received in VPN instance **mvpn**.
Total 2 data-groups for 8 entries	A total of 2 data groups, associated with 8 (S, G) entries.
Total 2 data-groups and 8 entries matched	A total of 2 matching data groups, associated with 8 matching (S, G) entries.
Data-group	IP address of the received data group.
Sender	BGP peer address of the PE device that sent the data group.
Reference count	Number of (S, G) entries that use the data group in the VPN instance.
Active count	Number of active (S, G) entries (entries with receivers) that use the data group in the VPN instance.
expires	Remaining time for the (S, G) entry that uses the data group in the VPN instance.

display multicast-vpn ipv6 data-group send

Use **display multicast-vpn ipv6 data-group send** to display information about data groups for IPv6 multicast transmission that are sent in a VPN instance.

Syntax

display multicast-vpn vpn-instance *vpn-instance-name* **ipv6 data-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [*mask-length*] | *vpn-group-address* [*mask-length*]] *

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.

group *group-address*: Specifies a data group by its IP address in the range of 224.0.1.0 to 239.255.255.255.

reuse *interval*: Specifies an interval during which data group reuses occur, in the range of 1 to 2147483647 seconds.

vpn-source-address: Specifies an IPv6 multicast source address of the specified VPN instance.

vpn-group-address: Specifies an IPv6 multicast group address of the specified VPN instance. The value range for this argument is FFxy::/16, where "x" and "y" represent any hexadecimal numbers from 0 to F.

mask-length: Specifies a mask length of the specified IPv6 multicast source or IPv6 multicast group address. For the IPv6 multicast source address, the value range for this argument is 8 to 128, and the default is 128. For the IPv6 multicast group address, the value range for this argument is 0 to 128, and the default is 128.

Examples

Display information about data groups for IPv6 multicast transmission that are sent in VPN instance **mvpn**.

```
<Sysname> display multicast-vpn vpn-instance mvpn ipv6 data-group send
MVPN data-group information sent by VPN instance: mvpn
Total 2 data-groups for 6 entries
Total 2 data-groups and 6 entries matched

Reference count of 226.1.1.0: 3
(192::1, ff1e::1)
switch time: 00:00:21
(192::1, ff1e::2)
switch time: 00:00:21
(192::1, ff1e::3)
 switch time: 00:00:05
Reference count of 226.1.1.1: 3
(192::2, ff1e::4)
switch time: 00:00:21
(192::2, ff1e::5)
switch time: 00:00:05
(192::2, ff1e::6)
 switch time: 00:00:21
```

Display reuse information about data groups for IPv6 multicast transmission that are sent in VPN instance **mvpn** within 30 seconds.

```
<Sysname> display multicast-vpn vpn-instance mvpn ipv6 data-group send reuse 30
MVPN data-group information sent by VPN instance: mvpn
Total 2 data-groups for 3 entries
Total 2 data-groups and 3 entries matched
```

```
Reuse count of 226.1.1.0: 1
Reuse count of 226.1.1.1: 1
Reuse count of 226.1.1.2: 1
```

Table 12 Command output

Field	Description
MVPN data-group information sent by VPN instance: mvpn	Information about data groups for IPv6 multicast transmission that are sent in VPN instance **mvpn**.
Total 2 data-groups for 6 entries	A total of 2 data groups, associated with 6 (S, G) entries.
Total 2 data-groups and 6 entries matched	A total of 2 matching data groups, associated with 6 matching (S, G) entries.
Reference count of 226.1.1.0	Number of (S, G) entries that use the data group in the VPN instance.
switch time	Switchover time of the (S, G) entry that uses the data group in the VPN instance.
Reuse count of 226.1.1.0	Number of times that the data group is reused during the specified length of time.

display multicast-vpn ipv6 default-group

Use **display multicast-vpn ipv6 default-group** to display information about default groups for IPv6 multicast transmission.

Syntax

display multicast-vpn [**vpn-instance** *vpn-instance-name*] **ipv6 default-group** { **local** | **remote** }

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 information about default groups of all VPN instances for IPv6 multicast transmission.

local: Specifies local default groups for IPv6 multicast transmission.

remote: Specifies remote default groups for IPv6 multicast transmission.

Examples

Display information about the local default group for IPv6 multicast transmission in each VPN instance.

```
<Sysname> display multicast-vpn ipv6 default-group local
MVPN local default-group information:
Group address    Source address   Interface     VPN instance
239.1.1.1        1.1.1.1          MTunnel0      mvpna
239.2.1.1        1.1.1.1          MTunnel1      mvpnb
239.3.1.1        --               MTunnel2      mvpnc
```

Display information about the remote default group for IPv6 multicast transmission in each VPN instance.

```
<Sysname> display multicast-vpn ipv6 default-group remote
MVPN remote default-group information:
Group address   Source address  Next hop         VPN instance
239.1.1.1       1.2.0.1         1.2.0.1          a
239.1.1.1       1.2.0.2         1.2.0.2          a
239.1.1.1       1.2.0.3         1.2.0.3          a
239.1.1.2       1.2.0.1         1.2.0.1          b
239.1.1.2       1.2.0.2         1.2.0.2          b
239.1.1.3       1.2.0.1         1.2.0.1          -
```

Table 13 Command output

Field	Description
Group address	IP address of the default group for IPv6 multicast transmission.
Source address	IP address of the MVPN source interface, which is used by the MTI as the source address to encapsulate IPv6 multicast packets of the VPN instance.
Interface	MTI interface.
Next hop	IP address of the next hop.
VPN instance	VPN instance to which the default group belongs.

dscp

Use **dscp** to set the DSCP value for outgoing data group switchover packets.

Use **undo dscp** to restore the default.

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value is 48 for outgoing data group switchover packets.

Views

MVPN view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value determines the packet transmission priority. A greater DSCP value represents a higher priority.

Examples

Set the DSCP value to 63 for outgoing data group switchover packets.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
```

```
[Sysname-mvpn-mvpn] dscp 63
```

log data-group-reuse

Use **log data-group-reuse** to enable data group reuse logging.

Use **undo log data-group-reuse** to disable data group reuse logging.

Syntax

log data-group-reuse

undo log data-group-reuse

Default

Data group reuse logging is disabled.

Views

MVPN IPv4 address family view

MVPN IPv6 address family view

Predefined user roles

network-admin

Examples

In MVPN IPv4 address family view of VPN instance **mvpn**, enable data group reuse logging.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv4
[Sysname-mvpn-mvpn-ipv4] log data-group-reuse
```

multicast rpf-proxy-vector compatible

Use **multicast rpf-proxy-vector compatible** to enable RPF vector compatibility.

Use **undo multicast rpf-proxy-vector compatible** to disable RPF vector compatibility.

Syntax

multicast rpf-proxy-vector compatible

undo multicast rpf-proxy-vector compatible

Default

RPF vector compatibility is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to work with other manufacturers' products on the RPF vector. You must configure this command on all HPE routers on the public network for multicast VPN inter-AS option B.

Examples

Enable RPF vector compatibility.

```
<Sysname> system-view
[Sysname] multicast rpf-proxy-vector compatible
```

multicast-vpn

Use **multicast-vpn** to create an MVPN for a VPN instance and enter its view, or enter the view of the existing MVPN.

Use **undo multicast-vpn** to delete configurations in MVPN view for a VPN instance.

Syntax

multicast-vpn vpn-instance *vpn-instance-name* **mode mdt**

undo multicast-vpn vpn-instance *vpn-instance-name*

Default

No MVPN exists.

Views

System 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.

mode: Specifies the mode of the MVPN.

mdt: Specifies the MDT mode.

Examples

Create an MDT-based MVPN for VPN instance **mvpn** and enter MVPN view.

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn]
```

rpf proxy vector

Use **rpf proxy vector** to enable the RPF vector feature.

Use **undo rpf proxy vector** to disable the RPF vector feature.

Syntax

rpf proxy vector

undo rpf proxy vector

Default

The RPF vector feature is disabled.

Views

MRIB view

Predefined user roles

network-admin

Usage guidelines

This feature enables PE devices to carry the RPF vector information in PIM join messages for other devices to perform RPF check on the messages.

You must enable this feature on PE devices (excluding the PE devices that do not have attached receivers) when you configure multicast VPN inter-AS option B.

Only the configuration made in MRIB view of a VPN instance takes effect. The configuration made in MRIB view on the public network does not take effect.

Examples

Enable the RPF vector feature for VPN instance **mvpn**.

```
<Sysname> system-view
[Sysname] multicast routing vpn-instance mvpn mode mdt
[Sysname-mrib-mvpn] rpf proxy vector
```

source

Use **source** to specify an MVPN source interface.

Use **undo source** to restore the default.

Syntax

source *interface-type interface-number*

undo source

Default

No MVPN source interface is specified.

Views

MVPN IPv4 address family view

MVPN IPv6 address family view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

For the PE device to obtain correct routing information, you must specify the interface used for establishing BGP peer relationship as the MVPN source interface.

For an MVPN that transmits both IPv4 and IPv6 multicast packets, you must specify the same MVPN source interface in MVPN IPv4 and IPv6 address family views.

Examples

In MVPN IPv4 address family view and IPv6 address family view of VPN instance **mvpn**, specify Loopback 1 as the MVPN source interface. (Loopback 1 is the source interface used for establishing BGP peer relationship.)

```
<Sysname> system-view
[Sysname] multicast-vpn vpn-instance mvpn mode mdt
[Sysname-mvpn-mvpn] address-family ipv4
[Sysname-mvpn-mvpn-ipv4] source loopback 1
[Sysname-mvpn-mvpn-ipv4] quit
[Sysname-mvpn-mvpn] address-family ipv6
```

```
[Sysname-mvpn-mvpn-ipv6] source loopback 1
```

New feature: EAP profiles

Configuring an EAP profile

About EAP profiles

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods.

Restrictions and guidelines

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

Prerequisites

Before you specify a CA certificate file, use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

Procedure

To configure an EAP profile:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an EAP profile and enter EAP profile view.	**eap-profile** *eap-profile-name*	N/A
3. Specify the EAP authentication method.	**method** { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }	By default, the EAP authentication method is MD5-challenge.
4. Specify a CA certificate file for EAP authentication.	**ca-file** *file-name*	By default, no CA certificate file is specified for EAP authentication. You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

Command reference

New command: ca-file

Use **ca-file** to specify a CA certificate file for EAP authentication.

Use **undo ca-file** to restore the default.

Syntax

ca-file *file-name*

undo ca-file

Default

No CA certificate file is specified for EAP authentication. The device does not verify the RADIUS server certificate during EAP authentication.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

file-name: Specifies a CA certificate file by its name, a case-sensitive string of 1 to 91 characters.

Usage guidelines

You must specify a CA certificate file to verify the RADIUS server certificate if the EAP authentication method is PEAP-GTC, PEAP-MSCHAPv2, TTLS-GTC, or TTLS-MSCHAPv2.

Before you specify a CA certificate file, you must use FTP or TFTP to transfer the CA certificate file to the root directory of the default storage medium on the device.

In an IRF fabric, make sure a CA certificate file already exists in the root directory of the default storage medium on the master device before you specify the file.

You can specify only one CA certificate file in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the CA certificate file, the new CA certificate file takes effect at the next server status detection.

Examples

In EAP profile **eap1**, specify CA certificate file **CA.der** for EAP authentication.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] ca-file CA.der
```

New command: eap-profile

Use **eap-profile** to create an EAP profile and enter its view, or enter the view of an existing EAP profile.

Use **undo eap-profile** to delete an EAP profile.

Syntax

eap-profile *eap-profile-name*

undo eap-profile *eap-profile-name*

Default

No EAP profiles exist.

Views

System view

Predefined user roles

network-admin

Parameters

eap-profile-name: Specifies the EAP profile name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

An EAP profile is a collection of EAP authentication settings, including the EAP authentication method and the CA certificate file to be used for some EAP authentication methods. You can use an EAP profile in a test profile for RADIUS server status detection.

You can specify an EAP profile in multiple test profiles.

You can configure a maximum of 16 EAP profiles.

Examples

Create an EAP profile named **eap1** and enter its view.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1]
```

Related commands

radius-server test-profile

New command: method

Use **method** to specify the EAP authentication method.

Use **undo method** to restore the default.

Syntax

method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

undo method

Default

MD5-challenge authentication is used.

Views

EAP profile view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5-challenge method.

peap-gtc: Specifies the PEAP-GTC method.

peap-mschapv2: Specifies the PEAP-MSCHAPv2 method.

ttls-gtc: Specifies the TTLS-GTC method.

ttls-mschapv2: Specifies the TTLS-MSCHAPv2 method.

Usage guidelines

You must specify an EAP authentication method that is supported by the RADIUS server to be detected.

You can specify only one EAP authentication method in an EAP profile. If you execute this command multiple times, the most recent configuration takes effect.

If you change the EAP authentication method, the new method takes effect in the next server status detection.

Examples

In EAP profile **eap1**, specify PEAP-GTC as the EAP authentication method.

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] method peap-gtc
```

Modified command: display radius scheme

Syntax

display radius scheme [*radius-scheme-name*]

Views

Any view

Change description

The **Probe eap-profile** field was added to the command output.

This field indicates the EAP profile used for RADIUS server status detection.

New feature: User aging for unauthenticated MAC authentication users

Configuring user aging for unauthenticated MAC authentication users

About user aging for unauthenticated MAC authentication users

User aging for unauthenticated MAC authentication users applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

Restrictions and guidelines

As a best practice, disable user aging for unauthenticated MAC authentication users unless you want to accommodate mobile users that move between ports.

Procedure

To configure user aging for unauthenticated MAC authentication users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the user aging timer for a type of MAC authentication VLAN.	**mac-authentication timer user-aging** { **critical-vlan** | **guest-vlan** } *aging-time-value*	By default, the user aging timer is 1000 seconds for all applicable types of MAC authentication VLANs.
3. Enter interface view.	**interface** *interface-type interface-number*	N/A
4. Enable user aging for unauthenticated MAC	**mac-authentication unauthenticated-user aging**	By default, user aging is enabled for unauthenticated MAC

Step	Command	Remarks
authentication users.	**enable**	authentication users.

Command reference

New command: mac-authentication unauthenticated-user aging enable

Use **mac-authentication unauthenticated-user aging enable** to enable user aging for unauthenticated MAC authentication users.

Use **undo mac-authentication unauthenticated-user aging enable** to disable user aging for unauthenticated MAC authentication users.

Syntax

mac-authentication unauthenticated-user aging enable

undo mac-authentication unauthenticated-user aging enable

Default

User aging is enabled for unauthenticated MAC authentication users.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

User aging for unauthenticated MAC authentication users applies to users added to a MAC authentication guest or critical VLAN because they have not been authenticated or have failed authentication.

When a user in one of those VLANs ages out, the device removes the user from the VLAN and deletes the MAC address entry for the user from the access port.

For users in one of those VLANs on one port to be authenticated successfully and come online on another port, enable this feature. In any other scenarios, disable this feature as a best practice.

Examples

Disable user aging for unauthenticated MAC authentication users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-authentication unauthenticated-user aging enable
```

Related commands

mac-authentication timer

Modified command: display mac-authentication

Syntax

display mac-authentication [**interface** *interface-type interface-number*]

Views

Any view

Change description

The fields in the following table were added to the command output:

Field	Description
User aging period for critical VLAN	Aging timer (in seconds) for users in critical VLANs.
User aging period for guest VLAN	Aging timer (in seconds) for users in guest VLANs.
User aging	Status of the aging feature for unauthenticated MAC authentication users on a port: • Enabled. • Disabled.

Modified command: mac-authentication timer (system view)

Old syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

New syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **user-aging** { **critical-vlan** | **guest-vlan** } *aging-time-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** | **user-aging** { **critical-vlan** | **guest-vlan** } }

Views

System view

Change description

The **user-aging** { **critical-vlan** | **guest-vlan** } *aging-time-value* parameters were added to this command.

user-aging: Sets the user aging timer for a type of MAC authentication VLAN.

critical-vlan: Specifies MAC authentication critical VLANs.

guest-vlan: Specifies MAC authentication guest VLANs.

aging-time-value: Sets the user aging timer. The value range is 60 to 2147483647 seconds.

New feature: User-specific MAC authentication offline detection

Configuring offline detection for a MAC authentication user

About user-specific offline detection in MAC authentication

In addition to port-based MAC authentication offline detection, you can configure offline detection parameters on a per-user basis, as follows:

- Set an offline detect timer specific to a user and control whether to use the ARP snooping or ND snooping table to determine the offline state of the user.

- If the ARP snooping or ND snooping table is used, the device searches the ARP snooping or ND snooping table before it checks for traffic from the user within the detection interval. If a matching ARP snooping or ND snooping entry is found, the device resets the offline detect timer and the user stays online. If the offline detect timer expires because the device has not found a matching snooping entry for the user or received traffic from the user, the device disconnects the user.
- If the ARP or ND snooping table is not used, the device disconnects the user if it has not received traffic from that user before the offline detect timer expires.

When disconnecting the user, the device also notifies the RADIUS server (if any) to stop user accounting.

- Skip offline detection for the user. You can choose this option if the user is a dumb terminal. A dumb terminal might fail to come online again after it is logged off by the offline detection feature.

The device uses the offline detection settings for a user in the following sequence:

1. User-specific offline detection settings.
2. Offline detection settings assigned to the user by the RADIUS server. The settings include the offline detect timer, use of the ARP or ND snooping table in offline detection, and whether to ignore offline detection.
3. Port-based offline detection settings.

Restrictions and guidelines

The user-specific offline detection settings take effect on the online users immediately after they are configured.

Prerequisites

For the user-specific offline detection settings to take effect on a user, make sure the MAC authentication offline detection feature is enabled on the user's access port.

Procedure

To configure MAC authentication offline detection for a user:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure MAC authentication offline detection for a user.	**mac-authentication offline-detect mac-address** *mac-address* { **ignore** | **timer** *offline-detect-value* [**check-arp-or-nd-snooping**] }	By default, offline detection settings configured on access ports take effect and the offline detect timer set in system view is used.

Command reference

mac-authentication offline-detect mac-address

Use **mac-authentication offline-detect mac-address** to configure MAC authentication offline detection for a MAC authentication user.

Use **undo mac-authentication offline-detect mac-address** to restore the default.

Syntax

mac-authentication offline-detect mac-address *mac-address* { **ignore** \| **timer** *offline-detect-value* [**check-arp-or-nd-snooping**] }

undo mac-authentication offline-detect mac-address *mac-address*

Default

The offline detection settings configured on access ports take effect and the offline detect timer set in system view is used.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address: Specifies a MAC address in the format of H-H-H, excluding multicast, all-zero, and all-F MAC addresses.

ignore: Skips offline detection for the specified user.

timer *offline-detect-value*: Specifies the offline detect timer for the specified user. The value range is 60 to 2147483647 seconds.

check-arp-or-nd-snooping: Uses the ARP snooping or ND snooping table in offline detection to determine the offline state of the user.

Usage guidelines

Use this command to set offline detection parameters specific to a MAC authentication user. To have this command take effect, you must make sure MAC authentication offline detection is enabled on the user's access port. The user-specific offline detection settings take effect on the online users immediately after they are configured.

Examples

Disable MAC authentication offline detection for the MAC authentication user with MAC address 000a-eb29-7511.

```
<Sysname> system-view
[Sysname] mac-authentication offline-detect mac-address 000a-eb29-7511 ignore
```

Enable MAC authentication offline detection for the MAC authentication user with MAC address 000a-eb29-7511, and set the offline detect timer to 24 hours.

```
<Sysname> system-view
[Sysname] mac-authentication offline-detect mac-address 000a-eb29-7511 timer 86400
```

Related commands

display mac-authentication connection

mac-authentication offline-detect enable

mac-authentication timer (system view)

Modified command: display mac-authentication connection

Syntax

display mac-authentication connection [**open**] [**interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *user-name*]

Views

Any view

Change description

The **Offline detection** field was added to the command output. The following are values for this field:

- **Ignore (command-configured)**—The device does not perform offline detection for the user. The setting was configured from the CLI.
- ***timer* (command-configured)**—Represents the offline detect timer setting configured from the CLI.
- **Ignore (server-assigned)**—The device does not perform offline detection for the user. The setting was assigned by a RADIUS server.
- ***timer* (server-assigned)**—Represents the offline detect timer setting assigned by a RADIUS server.

New feature: VLAN check bypass for the port security MAC move feature

Enabling VLAN check bypass for the port security MAC move feature

About VLAN check bypass

VLAN check bypass enables a port to ignore the VLAN information in the packets that trigger 802.1X or MAC reauthentication for MAC move users.

The port from which the user moves is called the source port and the port to which the user moves is called the destination port.

On the destination port, an 802.1X or MAC authentication user will be reauthenticated in the VLAN authorized on the source port if the source port is enabled with MAC-based VLAN. If that VLAN is not permitted to pass through on the destination port, reauthentication will fail. To avoid this situation, enable VLAN check bypass on the destination port.

Restrictions and guidelines

When you configure VLAN check bypass, follow these guidelines:

- To ensure a successful reauthentication, enable VLAN check bypass on a destination port if the source port is enabled with MAC-based VLAN.
- If the destination port is an 802.1X-enabled trunk port, you must configure it to send 802.1X protocol packets without VLAN tags. For more information, see 802.1X configuration in *Security Configuration Guide*.

Prerequisites

For VLAN check bypass to take effect, you must enable port security MAC move.

Procedure

To enable VLAN check bypass for MAC move users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable MAC move.	**port-security mac-move permit**	By default, MAC move is disabled.
3. Enter interface view.	**interface** *interface-type interface-number*	N/A
4. Enable VLAN check bypass for MAC move users.	**port-security mac-move bypass-vlan-check**	By default, the VLAN check bypass feature is disabled for MAC move users.

Command reference

New command: port-security mac-move bypass-vlan-check

Use **port-security mac-move bypass-vlan-check** to enable VLAN check bypass for MAC move users.

Use **undo port-security mac-move bypass-vlan-check** to disable VLAN check bypass for MAC move users.

Syntax

port-security mac-move bypass-vlan-check

undo port-security mac-move bypass-vlan-check

Default

VLAN check bypass is disabled for MAC move users. When reauthenticating a user that has moved to the port, the device examines whether the VLAN to which the user belongs is permitted by the port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable VLAN check bypass for MAC move users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-move bypass-vlan-check
```

Related commands

display port-security

dot1x eapol untag

port-security mac-move permit

Modified command: display port-security

Syntax

display port-security [**interface** *interface-type interface-number*]

Views

Any view

Change description

The **MAC-move VLAN check bypass** field was added to the command output to display the enabling status of the VLAN check bypass feature.

New feature: Specifying the source IP address for outgoing SCP packets

Specifying the source IP address for outgoing SCP packets

After you specify the source IP address for outgoing SCP packets on an SCP client, the client uses the specified IP address to communicate with the SCP server.

As a best practice, specify the IP address of a loopback or dialer interface as the source address of SCP packets for the following purposes:

- Ensuring the communication between the SCP client and the SCP server.
- Improving the manageability of SCP clients in authentication service.

To specify the source IP address for outgoing SCP packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the source address for outgoing SCP packets.	• Specify the source IPv4 address for outgoing SCP packets: **scp client source** { **interface** *interface-type interface-number* | **ip** *ip-address* } • Specify the source IPv6 address for outgoing SCP packets: **scp client ipv6 source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	By default, the source IP address for SCP packets is not configured. For outgoing IPv4 SCP packets, an SCP client uses the primary IPv4 address of the output interface in the matching routing entry as the source address of the packets. For outgoing IPv6 SCP packets, an SCP client automatically selects an IPv6 address as the source address of the packets in compliance with RFC 3484.
3. (Optional.) Display the source IP address configuration of the SCP client.	**display scp client source**	The command is available in any view.

Command reference

display scp client source

Use **display scp client source** to display the source IP address configuration of the SCP client.

Syntax

display scp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source IP address configuration of the SCP client.

```
<Sysname> display scp client source
The source IP address of the SCP client is 192.168.0.1.
The source IPv6 address of the SCP client is 2:2::2:2.
```

Related commands

scp client ipv6 source

scp client source

scp client ipv6 source

Use **scp client ipv6 source** to configure the source IPv6 address for SCP packets that are sent by the SCP client.

Use **undo scp client ipv6 source** to restore the default.

Syntax

scp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo scp client ipv6 source

Default

The source IPv6 address for outgoing SCP packets is not configured. The SCP client automatically selects an IPv6 address for outgoing SCP packets in compliance with RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client selects the interface's address that most specifically matches the destination address of outgoing SCP packets as the source address of the SCP packets.

ipv6 *ipv6-address*: Specifies a source IPv6 address.

Usage guidelines

This command takes effect on all IPv6 SCP connections. The source IPv6 address specified in the **scp ipv6** command takes effect only on the current IPv6 SCP connection. If you specify the source IPv6 address in both this command and the **scp ipv6** command, the source IPv6 address specified in the **scp ipv6** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **2:2::2:2** as the source IPv6 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client ipv6 source ipv6 2:2::2:2
```

Related commands

display scp client source

scp client source

Use **scp client source** to configure the source IPv4 address for SCP packets that are sent by the SCP client.

Use **undo scp client source** to restore the default.

Syntax

scp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo scp client source

Default

The source IPv4 address for outgoing SCP packets is not configured. The SCP client uses the primary IPv4 address of the output interface in the matching route as the source IPv4 address for outgoing SCP packets.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface by its type and number. The SCP client uses the primary IPv4 address of the interface as the source address of outgoing SCP packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command takes effect on all SCP connections. The source IPv4 address specified in the **scp** command takes effect only on the current SCP connection. If you specify the source IPv4 address in both this command and the **scp** command, the source IPv4 address specified in the **scp** command takes effect.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify **192.168.0.1** as the source IPv4 address for SCP packets.

```
<Sysname> system-view
[Sysname] scp client source ip 192.168.0.1
```

Related commands

display scp client source

New feature: Configuring the link-up delay timer

Configuring the link-up delay timer

Configuration restrictions and guidelines

If the **distribute** keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

If you specify the **distribute** keyword in an RRPP network implementing loading balancing, you must configure the link-up delay timer for each RRPP domain for the timer to take effect. If you set different timer values for different RRPP domains, the smallest timer value takes effect.

Configuration procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RRPP domain view.	**rrpp domain** *domain-id*	N/A
3. Set the link-up delay timer for the RRPP domain.	**linkup-delay-timer** *delay-time* [**distribute**]	By default, the link-up delay timer value is 0 seconds, and the **distribute** keyword is not specified.

Command reference

linkup-delay-timer

Use **linkup-delay-timer** to set the link-up delay timer.

Use **undo linkup-delay-timer** to restore the default.

Syntax

linkup-delay-timer *delay-time* [**distribute**]

undo linkup-delay-timer

Default

The link-up delay timer is 0 seconds, and the **distribute** keyword is not specified.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

delay-time: Specifies the link-up delay timer in the range of 0 to 30 seconds.

distribute: Enables all nodes in the RRPP domain to learn the link-up delay timer value.

Usage guidelines

The link-up delay timer prevents frequent switchover of RRPP traffic forwarding paths caused by unstable RRPP port states.

You can configure this command on any node in an RRPP domain, but this command can take effect only on the master node.

If the **distribute** keyword is not specified, the link-up delay timer value cannot be greater than the Fail timer value minus twice the Hello timer value.

Examples

Set the link-up delay timer to 10 seconds for RRPP domain 1.

```
<Sysname> system
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] linkup-delay-timer 10
```

Related commands

timer

New feature: Recording DHCPv6 snooping prefix entries on an interface

Enabling recording DHCPv6 snooping prefix entries on an interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	This interface must connect to the DHCPv6 client.
3. Enable recording DHCPv6 snooping prefix entries.	**ipv6 dhcp snooping pd binding record**	By default, recording of DHCPv6 snooping prefix entries is disabled.

Command reference

ipv6 dhcp snooping pd binding record

Use **ipv6 dhcp snooping pd binding record** to enable recording DHCPv6 snooping prefix entries.

Use **undo ipv6 dhcp snooping pd binding record** to disable recording DHCPv6 snooping prefix entries.

Syntax

ipv6 dhcp snooping pd binding record

undo ipv6 dhcp snooping pd binding record

Default

Recording of DHCPv6 snooping prefix entries is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN view

Predefined user roles

network-admin

Usage guidelines

This command enables DHCPv6 snooping to record IPv6 prefix-to-port information of the DHCPv6 clients (called DHCPv6 snooping prefix entries). When IP source guard (IPSG) is configured on the DHCP snooping device, IPSG can generate dynamic bindings based on the DHCP snooping prefix entries to filter out illegitimate packets.

Examples

Enable DHCPv6 snooping prefix entries on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname]interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping pd binding record
```

Related commands

display ipv6 dhcp snooping pd binding

display ipv6 dhcp snooping pd binding

Use **display ipv6 dhcp snooping pd binding** to display DHCPv6 snooping prefix entries.

Syntax

display ipv6 dhcp snooping pd binding [**prefix** *prefix*/*prefix-length* [**vlan** *vlan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

prefix *prefix*/*prefix-length*: Specifies an IPv6 prefix with its length. The value range for the *prefix-length* argument is 1 to 128.

vlan *vlan-id*: Specifies the ID of the VLAN where the IPv6 prefix resides. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

This command takes effect only after you execute the **ipv6 dhcp snooping pd binding record** command on the port directly connecting to the clients.

If you do not specify any parameters, this command displays all DHCPv6 snooping prefix entries.

Examples

Display all DHCPv6 snooping prefix entries.

```
<Sysname> display ipv6 dhcp snooping pd binding
1 DHCPv6 snooping PD entries found.
IPv6 prefix      Lease       VLAN SVLAN Interface
================ =========== ==== ===== ========================
1:2::/64         54          2    N/A   GigabitEthernet1/0/1
```

Table 14 Command output

Field	Description
DHCPv6 snooping PD entries found.	Total number of DHCPv6 snooping prefix entries.
IPv6 prefix	IPv6 prefix assigned to the DHCPv6 client.
Lease	Remaining lease duration in seconds.
VLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the outer VLAN tag. Otherwise, it identifies the VLAN where the port connecting the DHCPv6 client resides.
SVLAN	When both DHCPv6 snooping and QinQ are enabled or the DHCPv6 packet contains two VLAN tags, this field identifies the inner VLAN tag. Otherwise, it displays **N/A**.

Field	Description
Interface	Port connecting to the DHCPv6 client.

Related commands

ipv6 dhcp snooping pd binding record

reset ipv6 dhcp snooping pd binding

reset ipv6 dhcp snooping pd binding

Use **reset ipv6 dhcp snooping pd binding** to clear DHCPv6 snooping prefix entries.

Syntax

reset ipv6 dhcp snooping pd binding { **all** | **prefix** *prefix*/*prefix-length* [**vlan** *vlan-id*] }

Views

User view

Predefined user roles

network-admin

Parameters

all: Clears all DHCPv6 snooping prefix entries.

prefix *prefix*/*prefix-length*: Clears DHCPv6 snooping entries for the specified IPv6 prefix. The value range for the *prefix-length* argument is 1 to 128.

vlan *vlan-id*: Clears DHCPv6 snooping prefix entries for the specified VLAN. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

This command applies to all slots on a distributed device.

If you do not specify any parameters, this command clears all DHCPv6 snooping prefix entries.

Examples

Clear DHCPv6 snooping prefix entries for 1:2::/64.

```
<Sysname> reset ipv6 dhcp snooping pd binding prefix 1:2::/64
```

Related commands

display ipv6 dhcp snooping pd binding

New feature: Setting the interface-specific aging timer for ND entries in stale state

Setting the interface-specific aging timer for ND entries in stale state

ND entries in stale state have an aging timer. If an ND entry in stale state is not refreshed before the timer expires, the ND entry changes to the delay state. If it is still not refreshed in 5 seconds, the ND entry changes to the probe state, and the device sends an NS message three times. If no response is received, the device deletes the ND entry.

Configuration restrictions and guidelines

You can set the aging timer for ND entries in stale state in system view and interface view. For ND entries in stale state on an interface, the aging timer in interface view has higher priority than the aging timer in system view.

Configuration procedure

To set the aging timer for ND entries in stale state:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the aging timer for ND entries in stale state on the interface.	**ipv6 neighbor timer stale-aging** *aging-time*	By default, the aging timer of ND entries in stale state is not configured on an interface. The aging timer is determined by the configuration of the **ipv6 neighbor stale-aging** command in system view.

Command reference

ipv6 neighbor timer stale-aging

Use **ipv6 neighbor timer stale-aging** to set the aging timer for ND entries in stale state on an interface.

Use **undo ipv6 neighbor timer stale-aging** to restore the default.

Syntax

ipv6 neighbor timer stale-aging *aging-time*

undo ipv6 neighbor timer stale-aging

Default

The aging timer of ND entries in stale state is not configured on an interface. The aging timer is determined by the configuration of the **ipv6 neighbor stale-aging** command in system view.

Views

Layer 3 Ethernet interface/subinterface view

Layer 3 aggregate interface/subinterface view

VLAN interface view

Tunnel interface view

Predefined user roles

network-admin

Parameters

aging-time: Specifies the aging timer in minutes for ND entries in stale state, in the range of 1 to 1440.

Usage guidelines

This aging timer applies to ND entries in stale state on the interface. If an ND entry in stale state is not updated before the timer expires, it changes to the delay state. If it is still not updated in 5 seconds, the ND entry changes to the probe state. The device sends an NS message for probe and a maximum of three attempts is allowed. If no response is received, the device deletes the ND entry.

You can set the aging timer for ND entries in stale state in system view and interface view. For ND entries in stale state on an interface, the aging timer in interface view has higher priority than the aging timer in system view.

Examples

On VLAN-interface 2, set the aging timer to 200 minutes for ND entries in stale state.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 neighbor timer stale-aging 200
```

Related commands

ipv6 neighbor stale-aging

New feature: Enabling the Timestamps option encapsulation in outgoing TCP packets

Enabling the Timestamps option encapsulation in outgoing TCP packets

Devices at each end of the TCP connection can calculate the RTT value by using the TCP Timestamps option carried in TCP packets. For security purpose in some networks, you can disable this feature at one end of the TCP connection to prevent intermediate devices from obtaining the Timestamps option information.

To enable the timestamps option encapsulation in outgoing TCP packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the device to encapsulate the TCP Timestamps option in outgoing TCP packets.	**tcp timestamps enable**	By default, the TCP timestamps option is encapsulated in outgoing TCP packets.

Command reference

tcp timestamps enable

Use **tcp timestamps enable** to enable the device to encapsulate the TCP Timestamps option in outgoing TCP packets.

Use **undo tcp timestamps enable** to disable the device from encapsulating the TCP Timestamps option in outgoing TCP packets.

Syntax

tcp timestamps enable

undo tcp timestamps enable

Default

The TCP Timestamps option is encapsulated in outgoing TCP packets.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Devices at each end of the TCP connection can calculate the RTT value by using the TCP Timestamps option carried in TCP packets. For security purpose in some networks, you can disable the TCP Timestamps option encapsulation at one end of the TCP connection to prevent intermediate devices from obtaining the option information.

This command takes effect only on new connections that are established after you execute the command. Existing TCP connections are not affected.

Examples

Enable the device to encapsulate the TCP Timestamps option in outgoing TCP packets.

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

```
[Sysname] undo tcp timestamps enable
```

New feature: Setting the Telnet service port number

Setting the Telnet service port number

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the IPv4 Telnet service port number.	**telnet server port** *port-number*	By default, the IPv4 Telnet service port number is 23.
3. Set the IPv6 Telnet service port number.	**telnet server ipv6 port** *port-number*	By default, the IPv6 Telnet service port number is 23.

Command reference

telnet server ipv6 port

Use **telnet server ipv6 port** to specify the IPv6 Telnet service port number.

Use **undo telnet server ipv6 port** to restore the default.

Syntax

telnet server ipv6 port *port-number*

undo telnet server ipv6 port

Default

The IPv6 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv6 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv6 Telnet service port number to 1026.

```
<Sysname> system-view
[Sysname] telnet server ipv6 port 1026
```

telnet server port

Use **telnet server port** to specify the IPv4 Telnet service port number.

Use **undo telnet server port** to restore the default.

Syntax

telnet server port *port-number*

undo telnet server port

Default

The IPv4 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv4 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv4 Telnet service port number to 1025.

```
<Sysname> system-view
[Sysname] telnet server port 1025
```

New feature: USB-based automatic configuration

Using USB-based automatic configuration

About USB-based automatic configuration

USB-based automatic configuration enables the device to obtain a configuration file from a connected USB disk at startup.

After obtaining a configuration file, the device compares the file with its main startup configuration file. If the two files have the same settings, the device loads its main startup configuration file. If the two files have different settings, the device performs the following operations:

1. Identifies whether its main startup configuration file is using the same name as the obtained configuration file.
   - If yes, the device renames its main startup configuration file by using the *original base name*_**bak.cfg** name, and copies the obtained configuration file.
   - If not, the system uses the obtained configuration file to overwrite its main startup configuration file.
2. Loads the obtained configuration file.
   - If all commands in the obtained configuration file are successfully loaded, the device sets the obtained configuration file as the main startup configuration file.
   - If a command in the obtained configuration file fails, the device removes all loaded settings and searches for a local configuration file.
     - If a configuration file is found, the device loads the configuration file.
     - If no configuration file is found, the device finishes the automatic configuration process without loading any configurations.

Preparing the USB disk for automatic configuration

3. Prepare a USB disk that has only one partition.
4. Display the serial number of the device.

   display device manuinfo

   For more information about this command, see *Fundamentals Command Reference*.
5. Create a configuration file named *Device serial number***.cfg** or **autodeploy.cfg**, and save the file to the root directory of the file system on the USB disk.

   If a configuration file named *Device serial number***.cfg** coexists with the **autodeploy.cfg** file, the configuration file named *Device serial number***.cfg** is used.

Configuring and using USB-based automatic configuration

6. Enable USB-based automatic configuration on the device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable USB-based automatic configuration.	**autodeploy udisk enable**	By default, USB-based automatic configuration is enabled.
3. Save the running configuration.	**save**	A device reboot is required for USB-based automatic configuration. Save the running

Step	Command	Remarks
		configuration to ensure that the USB-based automatic configuration feature takes effect after a reboot.

7. Connect the USB disk to the USB1 interface on the device.

   The USB disk will be identified as **usba0:**.

8. Reboot the device and observe the LEDs of the device.
   - If the SYS LED flashes green quickly for 5 seconds, the automatic configuration succeeded. Proceed to step 5.
   - If the SYS LED flashes yellow quickly for 10 seconds, the automatic configuration failed. View the log file named *Fully qualified configuration file name***.log** in the USB disk root directory to locate and resolve the problem.
9. After the automatic configuration succeeded, use the **display current-configuration** command to verify that the configuration file has been loaded correctly.
10. Remove the USB disk.

    If you do not remove the USB disk, the device might start USB-based automatic configuration at the next reboot.

Command reference

autodeploy udisk enable

Use **autodeploy udisk enable** to enable USB-based automatic configuration.

Use **undo autodeploy udisk enable** to disable USB-based automatic configuration.

Syntax

autodeploy udisk enable

undo autodeploy udisk enable

Default

USB-based automatic configuration is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Disable USB-based automatic configuration.

```
<Sysname> system-view
[Sysname] undo autodeploy udisk enable
```

New feature: Resource monitoring

Configuring resource monitoring

About resource monitoring

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.

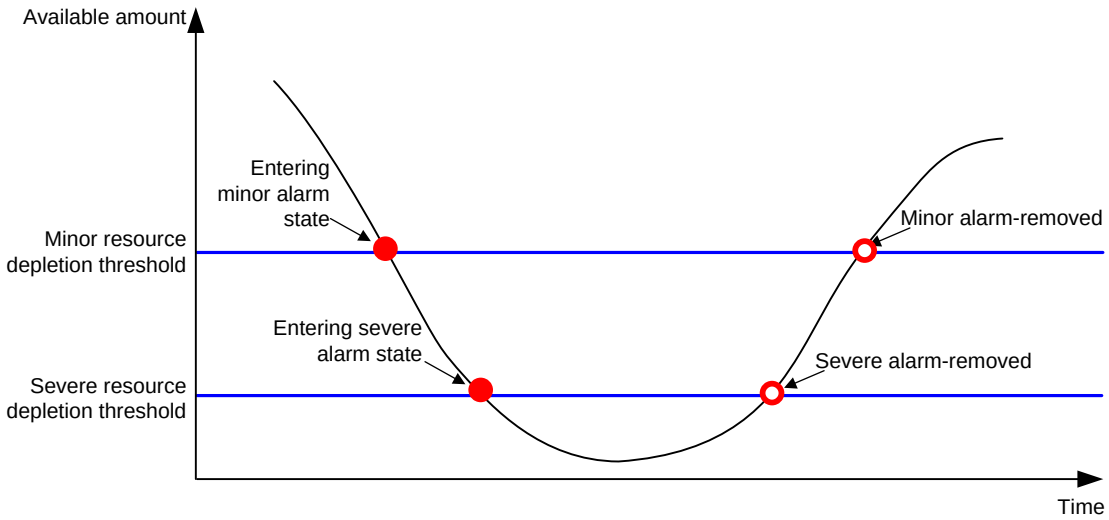
- If the available amount is equal to or less than the minor resource depletion threshold but greater than the severe resource depletion threshold, the resource type is in minor alarm state.
- If the available amount is equal to or less than the severe resource depletion threshold, the resource type 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 15 Resource depletion alarms and alarm-removed notifications



Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set resource depletion thresholds.	**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 sent to NETCONF, SNMP, and 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

display resource-monitor [**resource** *resource-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

resource *resource-name*: Specifies a resource type by its name. Table 15 lists the resource types that can be monitored.

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.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display ARP resource monitoring information.

```
<Sysname> display resource-monitor resource mac
Minor alarms resending: Enabled

Slot 1:
Resource                       Minor Severe Free/Total
                               (%)   (%)    (absolute)
mac                            20    10     32757/32768
```

Table 15 Command output

Field	Description
Minor alarms resending	Status of the minor resource depletion alarm resending feature, **Enabled** or **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.

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 sent to NETCONF, SNMP, and 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

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* **by-percent minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number*

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 15 lists the resource types that can be monitored.

Table 16 Resource types that can be monitored

Resource type	Description
agg_group	Aggregation group resources.
mac	MAC address table resources.
mqcin	Inbound MQC resources.
mqcout	Outbound MQC resources.
mqcvlan	VLAN-based MQC resources.
pfilterin	Inbound packet filter resources.
pfilterout	Outbound packet filter resources.

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

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

Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for ARP entry resources.

```
<Sysname> system-view
[Sysname] resource-monitor resource arp 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: PPPoE Relay

About PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) extends PPP by transporting PPP frames encapsulated in Ethernet over point-to-point links.

PPPoE specifies the methods for establishing PPPoE sessions and encapsulating PPP frames over Ethernet. PPPoE requires a point-to-point relationship between peers instead of a point-to-multipoint relationship as in multi-access environments such as Ethernet. PPPoE provides Internet access for the hosts in an Ethernet through a remote access device and implement access control, authentication, and accounting on a per-host basis. Integrating the low cost of Ethernet and scalability and management functions of PPP, PPPoE gained popularity in various application environments, such as residential access networks.

For more information about PPPoE, see RFC 2516.

PPPoE network structure

PPPoE uses the client/server model. The PPPoE client initiates a connection request to the PPPoE server. After session negotiation between them is complete, a session is established between them, and the PPPoE server provides access control, authentication, and accounting to the PPPoE client.

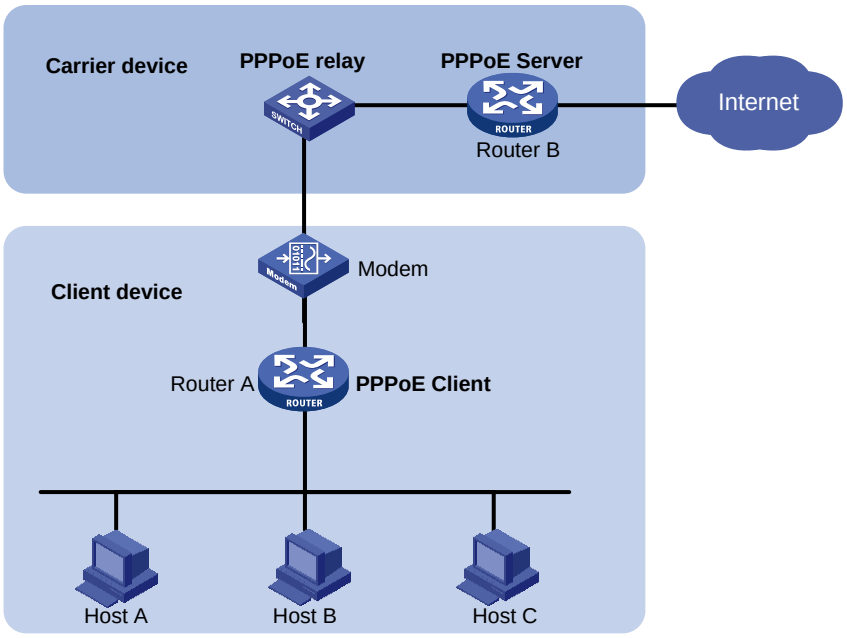
To granularly manage the PPPoE clients based on their location information, you can deploy a PPPoE relay between the PPPoE clients and PPPoE server.

PPPoE network structures are classified into router-initiated and host-initiated network structures depending on the starting point of the PPPoE session.

Router-initiated network structure

As shown in Figure 16, the PPPoE session is established between routers (Router A and Router B). All hosts share one PPPoE session for data transmission without being installed with PPPoE client software. This network structure is typically used by enterprises.

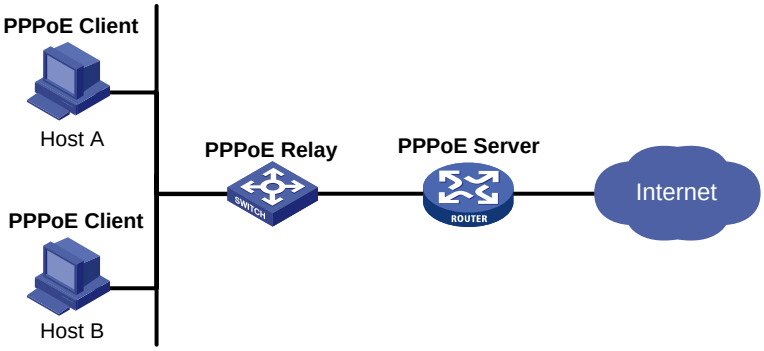
Figure 16 Router-initiated network structure



Host-initiated network structure

As shown in Figure 17, a PPPoE session is established between each host (PPPoE client) and the carrier router (PPPoE server). The service provider assigns an account to each host for billing and control. The host must be installed with PPPoE client software.

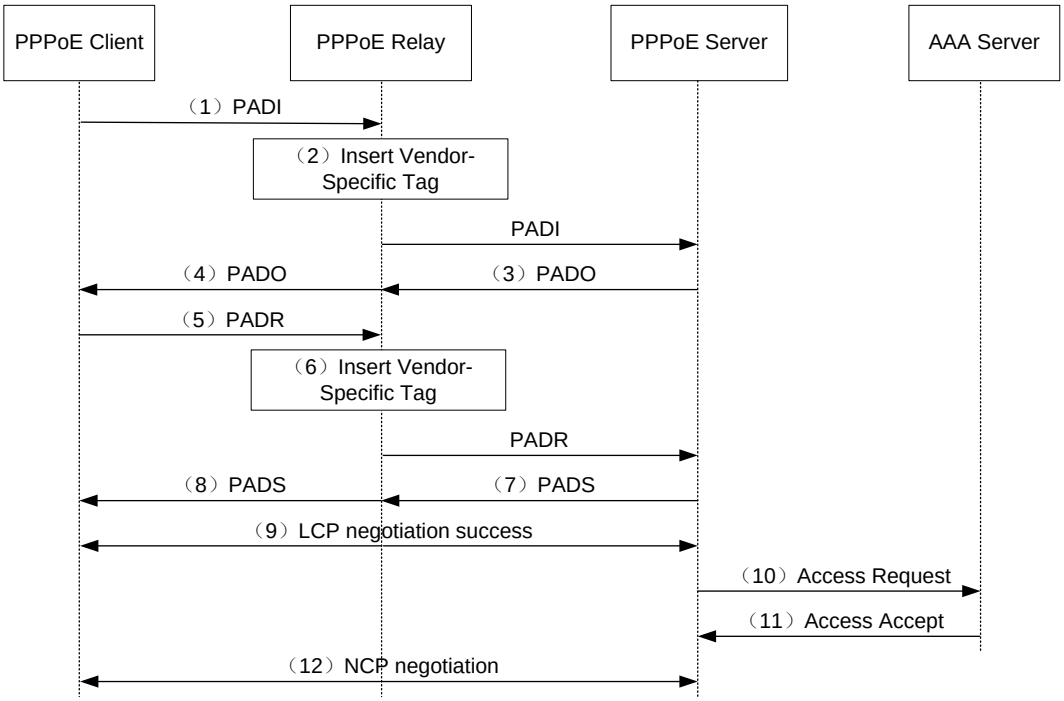
Figure 17 Host-initiated network structure



PPPoE relay fundamentals

The PPPoE relay controls protocol packet forwarding through monitoring the protocol packet exchange between the PPPoE client and the PPPoE server. Figure 18 shows the detailed process.

Figure 18 PPPoE client access procedure in a PPPoE relay network



1. The PPPoE client broadcasts a PADI packet.
2. When receiving the PADI packet, the PPPoE relay adds the vendor-specific tag field to the PADI packet and broadcasts the packet out of all trusted ports.

   The vendor-specific tag in a PPPoE packet identifies the location information (for example, the access port and VLANs) of a PPPoE client.
3. When receiving the PADI packets, the PPPoE server responds with a PADO packet to the PPPoE client.
4. When receiving the PADO packet, the PPPoE relay forwards the packet to the PPPoE client.
5. When receiving the PADO packet, the PPPoE client unicasts a PADR packet to the PPPoE server to apply for the PPPoE service.
6. When receiving the PADR packet, the PPPoE relay adds the vendor-specific tag to the packet and searches for an outgoing interface based on the destination MAC address of the PADR packet.
   - If the outgoing interface is a trusted port, the PPPoE relay forwards the packet out of the port.
   - If the outgoing interface is an untrusted port, the PPPoE relay drops the PADR packet.
7. When receiving the PADR packet, the PPPoE server assigns a session ID to the PPPoE client and binds the session ID to the vendor-specific tag. Then, the PPPoE server responds with a PADS packet to the PPPoE client.
8. When receiving the PADS packet, the PPPoE relay forwards the packet to the PPPoE client.
9. When receiving the PADS packet, the PPPoE client starts the LCP negotiation and authentication with the PPPoE server.
10. During the authentication phase, the PPPoE server will send the location information, username, and password of the PPPoE client to the RADIUS server for authentication.
11. The RADIUS server compares the location information, username, and password saved in the database with those of the PPPoE client. If they match, the PPPoE client passes the authentication.

12. After the PPPoE client passes authentication, the PPPoE client starts NCP negotiation with the PPPoE server. After the NCP negotiation succeeds, the PPPoE client successfully comes online.

Protocols and standards

RFC 2516: A Method for Transmitting PPP Over Ethernet (PPPoE)

Restrictions and guidelines: PPPoE configuration

The PPPoE relay supports the following interface views:

- Layer 2 Ethernet interface view
- Layer 2 aggregate interface view

Configuring the PPPoE relay

Enabling the PPPoE relay function

About the PPPoE relay function

For the PPPoE relay-related configurations to take effect, you must enable the PPPoE relay function.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the PPPoE relay function.	**pppoe-relay enable**	By default, the PPPoE relay function is disabled.

Configuring PPPoE relay trusted ports

About PPPoE relay trusted ports

A PPPoE relay-enabled device processes PPPoE protocol packets as follows:

- When receiving PADI, PADR, and PADT on untrusted ports, the device can forward the packets out of only the trusted ports.
- When receiving PADO and PADS packets on untrusted ports, the device directly drops the packets.
- When receiving PADO, PADS, and PADT packets on trusted ports, the device can forward the packets out of any port.
- When receiving PADI and PADR packets on trusted ports, the device can forward the packets out of only the trusted ports.

For a PPPoE relay to correctly forward and process PPPoE protocol packets, you must configure the PPPoE server-facing interfaces on the PPPoE relay as trusted ports, and configure the PPPoE client-facing interfaces on the PPPoE relay as untrusted ports.

Restrictions and guidelines

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member port joins the aggregation group.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the interface as a PPPoE relay trusted port.	**pppoe-relay trust**	By default, an interface is not configured as a PPPoE relay trusted port.

Enabling an interface to strip the vendor-specific tags of the PPPoE server-side packets

About stripping the vendor-specific tags of the PPPoE server-side packets

When the PPPoE relay receives PADO and PADS packets from the PPPoE server on a PPPoE relay trusted port with this feature enabled, the PPPoE relay strips the vendor-specific tags of the packets before forwarding the packets.

Restrictions and guidelines

This feature takes effect only on packets received on PPPoE relay trusted ports.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable the interface to strip the vendor-specific tags of the PPPoE server-side packets.	**pppoe-relay server-information vendor-specific strip**	By default, the function of stripping vendor-specific tags of the PPPoE server-side packets is disabled.

Configuring the circuit ID and remote ID padding formats for the client-side PPPoE packets on the PPPoE relay

About the circuit ID and remote ID padding formats for the client-side PPPoE packets on the PPPoE relay

When the PPPoE relay receives PPPoE packets from the PPPoE client, the PPPoE relay pads the circuit ID and remote ID with the contents in the format configured by using this command.

Both the circuit ID and remote ID are of up to 63 characters. When the content to be padded exceeds 63 characters, the first 63 characters are padded.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Configure the circuit ID and remote ID padding formats for the client-side PPPoE packets on the PPPoE relay.	**pppoe-relay client-information format** { **circuit-id** | **remote-id** } { **ascii** | **hex** | **user-defined** *text* }	By default, both the circuit ID padding format and the remote ID padding format for the client-side PPPoE packets are the ASCII string format on the PPPoE relay.

Configuring the vendor-specific tag processing policy for the client-side PPPoE packets on the PPPoE relay

About the vendor-specific tag processing policy for the client-side PPPoE packets on the PPPoE relay

When the PPPoE relay receives PADI or PADR packets, the PPPoE relay processes the packet according to whether the packets carry the vendor-specific tag and the configured vendor-specific tag processing policy. Then, the PPPoE relay sends the packets to the PPPoE server. Table 16 shows the detailed process.

Table 17 Vendor-specific tag processing policy on the PPPoE relay

Whether the received packets carry the vendor-specific tag	Vendor-specific tag processing policy	Processing for packets on the PPPoE relay
The received packets carry vendor-specific tag	Drop	Strips the vendor-specific tag and then forwards the packets.
	Keep	Keeps the vendor-specific tag unchanged and forwards the packets.
	Replace	Pads the vendor-specific tag in the configured format, replaces the original vendor-specific tag with the new vendor-specific tag, and forwards the packets.
The received packets do not carry vendor-specific tag	Drop	Directly forwards the packets.
	Keep	Directly forwards the packets.
	Replace	Pads the vendor-specific tag in the configured format, adds the new vendor-specific tag to the packets, and forwards the packets.

Restrictions and guidelines

This feature can be configured both in system view and in interface view. The configuration in system view takes effect on all interfaces. The configuration in interface view takes effect only on the current interface. The configuration in interface view takes precedence over the configuration in system view.

The processing policy takes effect only on incoming packets of interfaces.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Configuring the global vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Configure the global vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay.	**pppoe-relay client-information strategy** { **drop** | **keep** | **replace** }	By default, the global vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay is replace.

Configuring an interface-level vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the vendor-specific tag processing policy for the client-side PADI and PADR packets for the interface on the PPPoE relay.	**pppoe-relay client-information strategy** { **drop** | **keep** | **replace** }	By default, no vendor-specific tag processing policy for the client-side PADI and PADR packets is configured for an interface on the PPPoE relay.

Display and maintenance commands for PPPoE

Display and maintenance commands for PPPoE relay

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

Task	Command
Display the vendor-specific tag processing configuration for client-side packets on the PPPoE relay.	**display pppoe-relay client-information** { **format** | **strategy** }
Display packet statistics for the PPPoE relay.	**display pppoe-relay statistics** [**interface** *interface-type interface-number*]
Clear packet statistics for the PPPoE relay.	**reset pppoe-relay statistics**

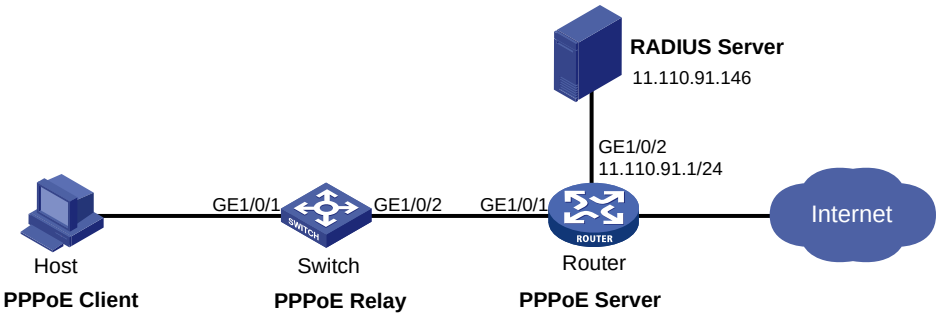
PPPoE configuration examples

Example: Configuring PPPoE relay

Network configuration

As shown in Figure 19, the host uses the PPPoE access method to connect to the router through the switch. The switch acts as the PPPoE relay. The router acts as the PPPoE server and assigns IPv4 addresses to the PPPoE client through a PPP address pool.

Figure 19 Network diagram



Procedure

1. Configure the switch as the PPPoE relay:

   # Enable the PPPoE relay function.

   ```
   <Switch> system-view
   [Switch] pppoe-relay enable
   ```

   # Configure the server-facing interface GigabitEthernet 1/0/2 as a PPPoE relay trusted port.

   ```
   [Switch] interface GigabitEthernet 1/0/2
   [Switch-GigabitEthernet1/0/2] pppoe-relay trust
   ```

2. Configure the router as a PPPoE server:

   # Create a PPPoE user.

   ```
   <Router> system-view
   [Router] local-user user1 class network
   [Router-luser-network-user1] password simple pass1
   [Router-luser-network-user1] service-type ppp
   [Router-luser-network-user1] quit
   ```

   # Configure Virtual-Template 1 to use CHAP for authentication and use a PPP address pool for IP address assignment. Set the DNS server IP address for the peer.

   ```
   [Router] interface virtual-template 1
   [Router-Virtual-Template1] ppp authentication-mode chap domain system
   [Router-Virtual-Template1] ppp chap user user1
   [Router-Virtual-Template1] remote address pool 1
   [Router-Virtual-Template1] ppp ipcp dns 8.8.8.8
   [Router-Virtual-Template1] quit
   ```

   # Configure a PPP address pool that contains nine assignable IP addresses, and configure a gateway address for the PPP address pool.

   ```
   [Router] ip pool 1 1.1.1.2 1.1.1.10
   [Router] ip pool 1 gateway 1.1.1.1
   ```

   # Enable the PPPoE server on GigabitEthernet 1/0/1, and bind the interface to Virtual-Template 1.

   ```
   [Router] interface gigabitethernet 1/0/1
   [Router-GigabitEthernet1/0/1] pppoe-server bind virtual-template 1
   [Router-GigabitEthernet1/0/1] quit
   ```

   # Configure the default ISP domain (**system**) to use the RADIUS scheme for authentication, authorization, and accounting.

   ```
   [Router] domain system
   [Router-isp-system] authentication ppp radius-scheme rs1
   [Router-isp-system] authorization ppp radius-scheme rs1
   ```

```
[Router-isp-system] accounting ppp radius-scheme rs1
[Router-isp-system] quit
```

Configure a RADIUS scheme, and specify the primary authentication server and the primary accounting server.

```
[Router] radius scheme rs1
[Router-radius-rs1] primary authentication 11.110.91.146
[Router-radius-rs1] primary accounting 11.110.91.146
```

Set the shared key for secure communication with the authentication and accounting servers to **expert** in plain text.

```
[Router-radius-rs1] key authentication simple expert
[Router-radius-rs1] key accounting simple expert
[Router-radius-rs1] quit
```

3. Configure the RADIUS server:
   a. Configure the authentication and accounting passwords as **expert**.
   b. Add a PPPoE user with username **user1** and password **123456**.

   For more information, see the user manual for the RADIUS server.

Verifying the configuration

Install the PPPoE client software and configure the username and password (**user1** and **pass1** in this example) on the hosts. Then, the hosts can use PPPoE to access the Internet through the router.

Command reference

display pppoe-relay client-information

Use **display pppoe-relay client-information** to display the vendor-specific tag processing configuration for client-side packets on the PPPoE relay.

Syntax

display pppoe-relay client-information { **format** | **strategy** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

format: Displays the format configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

strategy: Displays the policy configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

Examples

Display the format configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

```
<Sysname> display pppoe-relay client-information format
The current client-information format:
Circuit ID: ASCII
Remote ID: ASCII
```

Display the policy configuration for the vendor-specific tag processing for client-side packets on the PPPoE relay.

```
<Sysname> display pppoe-relay client-information strategy
The current global client-information strategy: Replace
The current interface client-information strategy:
  Interface                     Strategy
  GigabitEthernet1/0/1            Keep
  GigabitEthernet1/0/2            Drop
```

Table 18 Command output

Field	Description
The current client-information format	Circuit ID and remote ID padding formats in the vendor-specific tag: • **ASCII**—ASCII string padding format. • **Hex**—Hexadecimal padding format. • **User-defined**—User-defined padding format.
The current global client-information strategy	Global vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay: • **Drop**—Strips the vendor-specific tag from the PADI or PADR packets. • **Keep**—Keeps the vendor-specific tag unchanged. • **Replace**—Pads the vendor-specific tag in the configured padding format.
The current interface client-information strategy	Interface-level vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay.
Interface	Interface name. This field displays only the interfaces whose processing policies are different from the global processing policy.
Strategy	Vendor-specific tag processing policy for the client-side PADI and PADR packets of the interface on the PPPoE relay: • **Drop**—Strips the vendor-specific tag from the PADI or PADR packets. • **Keep**—Keeps the vendor-specific tag unchanged. • **Replace**—Pads the vendor-specific tag in the configured padding format.

Related commands

pppoe-relay client-information format

pppoe-relay client-information strategy

display pppoe-relay statistics

Use **display pppoe-relay statistics** to display packets statistics for the PPPoE relay.

Syntax

display pppoe-relay statistics [**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.

Usage guidelines

When this command is executed, this command displays statistics only for packets with non-zero packet counts.

Examples

Display packet statistics on GigabitEthernet 1/0/1.

```
<Sysname> display pppoe-relay statistics interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
  Packets received:
    ALL = 5 PADI = 5 PADO = 0 PADR = 0 PADS = 0 PADT = 0
  Packets sent:
    ALL = 5 PADI = 0 PADO = 5 PADR = 0 PADS = 0 PADT = 0
  Packets dropped:
    Server responses from untrusted ports = 0
    Client requests towards untrusted ports = 0
    Malformed PPPoE Discovery packets = 0
```

Table 19 Command output

Field	Description
Interface	Statistics on an interface.
Packets received	Incoming packet statistics of the interface: • **ALL**—Number of all PAD packets. • **PADI**—Number of PADI packets. • **PADO**—Number of PADO packets. • **PADR**—Number of PADR packets. • **PADS**—Number of PADS packets. • **PADT**—Number of PADT packets.
Packets sent	Outgoing packet statistics of the interface: • **ALL**—Number of all PAD packets. • **PADI**—Number of PADI packets. • **PADO**—Number of PADO packets. • **PADR**—Number of PADR packets. • **PADS**—Number of PADS packets. • **PADT**—Number of PADT packets.
Packets dropped	Dropped packets statistics of the interface.
Server responses from untrusted ports	Number of PADO and PADS packets dropped on untrusted ports.
Client requests towards untrusted ports	Number of PADR packets dropped by untrusted ports.

Related commands

reset pppoe-relay statistics

pppoe-relay client-information format

Use **pppoe-relay client-information format** to configure the circuit ID and remote ID padding formats for the client-side PPPoE packets on the PPPoE relay.

Use **undo pppoe-relay client-information format** to restore the default.

Syntax

pppoe-relay client-information format { **circuit-id** | **remote-id** } { **ascii** | **hex** | **user-defined** *text* }

undo pppoe-relay client-information format { **circuit-id** | **remote-id** }

Default

Both the circuit ID padding format and the remote ID padding format for the client-side PPPoE packets are the ASCII string on the PPPoE relay.

Views

System view

Predefined user roles

network-admin

Parameters

circuit-id: Specifies the circuit ID padding format.

remote-id: Specifies the remote ID padding format.

ascii: Specifies the ASCII string format. When this format is configured, **"**%portname:%svlan.%cvlan %sysname**"** is extracted and used as the circuit ID content, and **"**%mac**"** is used as the remote ID content. The circuit ID and remote ID are padded with the corresponding contents in the ASCII string format.

hex: Specifies the hexadecimal format. When this format is configured, **"**%length%port%svlan%cvlan**"** is extracted and used as the circuit ID content, and **"**%length%mac**"** is used as the remote ID content. The circuit ID and remote ID are padded with the corresponding contents in the hexadecimal format.

user-defined *text*: Specifies the user-defined format. The *text* argument is a case-sensitive string of 1 to 127 characters. When this format is configured, the corresponding information is extracted from the configured text and padded in the circuit ID and remote ID.

Usage guidelines

When the PPPoE relay receives PPPoE packets from the PPPoE client, the PPPoE relay pads the circuit ID and remote ID with the contents in the format configured by using this command.

Both the circuit ID and remote ID are of up to 63 characters. When the content to be padded exceeds 63 characters, the first 63 characters are padded.

When the user-defined format is used, the system automatically recognizes the escape keyword input by the user and translates it to the actual information. For more information about the supported escape keywords, see Table 19. For example, suppose the interface that receives packet on the PPPoE relay is Ethernet 0/0/0. In this case, you can input the escape keyword **%portname**. Then, the system automatically recognizes the escape keyword and translates the escape keyword into the actual port information Ethernet 0/0/0. For the system to correctly recognize the escape keywords, you must add the dollar sign (%) before each keyword. Otherwise, the system directly uses the input keyword and does not translate it. Non-escape keywords are directly used.

An integer can be added between the dollar sign (%) and the escape keyword. The integer specifies the width of the translated characters. When the translated characters do not reach the width specified by the integer, spaces are padded on the left to fill the width.

Table 20 Description of escape keywords supported by the user-defined format

Keyword	Description
sysname	System name of the PPPoE relay.

Keyword	Description
portname	Port name.
porttype	Port type.
slot	Slot number of the port.
subslot	Subslot number of the port.
port	Port number.
svlan	Outer VLAN ID.
cvlan	Inner VLAN ID.
mac	MAC address of the PPPoE relay.
Length	Length of the subsequent string. The padded content is of double digits. When the length is a single digit, one digit of 0 is padded on the left.

When you use different padding formats, the packet contents are different. For example, the contents of the circuit ID are as follows: the user access interface is Ethernet 0/0/0, the outer VLAN ID is 200, the inner VLAN ID is 100, and the system name of the PPPoE relay is Sysname. The contents of the remote ID are as follows: the MAC address of the PPPoE relay is 04f9-38a9-44b0.

When you use the ASCII string format, the contents are as follows:

```
Circuit ID: Ethernet0/0/0:200.100 Sysname
Remote ID: 04f9-38a9-44b0
```

When you use the hexadecimal format, the contents are as follows:

```
Circuit ID: 00 05 00 00 c8 00 64
Remote ID: 00 06 04 f9 38 a9 44 b0
```

When you use the user-defined format, the contents are as follows:

Configure the user-defined format "%portname:%svlan.%cvlan %sysname" for the circuit ID.

```
[Sysname] pppoe-relay client-information format circuit-id user-defined
"%portname:%svlan.%cvlan %sysname"
```

Configure the user-defined format %mac for the remote ID.

```
[Sysname] pppoe-relay client-information format remote-id user-defined "%mac"
```

Examples

Configure the circuit ID padding format as the ASCII string format for the client-side PPPoE packets on the PPPoE relay.

```
<Sysname> system-view
[Sysname] pppoe-relay client-information format circuit-id ascii
```

Related commands

display pppoe-relay client-information

pppoe-relay client-information strategy

pppoe-relay client-information strategy

Use **pppoe-relay client-information strategy** to configure the vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay.

Use **undo pppoe-relay client-information strategy** to restore the default.

Syntax

pppoe-relay client-information strategy { **drop** | **keep** | **replace** }

undo pppoe-relay client-information strategy

Default

The global vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay is replace.

No interface-level vendor-specific tag processing policy for the client-side PADI and PADR packets on the PPPoE relay is configured.

Views

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

drop: Strips the vendor-specific tag from the PADI or PADR packets.

keep: Keeps the vendor-specific tag unchanged.

replace: Pads the vendor-specific tag in the configured format.

Usage guidelines

This feature can be configured both in system view and in interface view. The configuration in system view takes effect on all interfaces. The configuration in interface view takes effect only on the current interface. The configuration in interface view takes precedence over the configuration in system view.

The processing policy takes effect only on incoming packets of interfaces.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Examples

Configure the global processing policy for the client-side PADI and PADR packets as drop on the PPPoE relay.

```
<Sysname> system-view
[Sysname] pppoe-relay client-information strategy drop
```

Related commands

display pppoe-relay client-information

pppoe-relay client-information format

pppoe-relay enable

Use **pppoe-relay enable** to enable the PPPoE relay function.

Use **undo pppoe-relay enable** to disable the PPPoE relay function.

Syntax

pppoe-relay enable

undo pppoe-relay enable

Default

The PPPoE relay function is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the PPPoE relay function.

```
<Sysname> system-view
[Sysname] pppoe-relay enable
```

pppoe-relay server-information vendor-specific strip

Use **pppoe-relay server-information vendor-specific strip** to enable an interface to strip the vendor-specific tags of the PPPoE server-side packets.

Use **undo pppoe-relay server-information vendor-specific strip** to disable an interface from stripping the vendor-specific tags of the PPPoE server-side packets.

Syntax

pppoe-relay server-information vendor-specific strip

undo pppoe-relay server-information vendor-specific strip

Default

The function of stripping vendor-specific tags of the PPPoE server-side packets is disabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

When the PPPoE relay receives PADO and PADS packets from the PPPoE server on a PPPoE relay trusted port with this feature enabled, the PPPoE relay strips the vendor-specific tags of the packets before forwarding the packets.

This command takes effect only on packets received on PPPoE relay trusted ports.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Examples

Enable GigabitEthernet 1/0/1 to strip the vendor-specific tags of the PPPoE server-side packets..

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-relay trust
[Sysname-GigabitEthernet1/0/1] pppoe-relay server-information vendor-specific strip
```

Related commands

pppoe-relay trust

pppoe-relay trust

Use **pppoe-relay trust** to configure an interface as PPPoE relay trusted port.

Use **undo pppoe-relay trust** to restore the default.

Syntax

pppoe-relay trust

undo pppoe-relay trust

Default

An interface is a PPPoE relay untrusted port.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Usage guidelines

A PPPoE relay-enabled device processes PPPoE protocol packets as follows:

- When receiving PADI, PADR, and PADT on untrusted ports, the device can forward the packets out of only the trusted ports.
- When receiving PADO and PADS packets on untrusted ports, the device directly drops the packets.
- When receiving PADO, PADS, and PADT packets on trusted ports, the device can forward the packets out of any port.
- When receiving PADI and PADR packets on trusted ports, the device can forward the packets out of only the trusted ports.

For a PPPoE relay to correctly forward and process PPPoE protocol packets, you must configure the PPPoE server-facing interfaces on the PPPoE relay as trusted ports, and configure the PPPoE client-facing interfaces on the PPPoE relay as untrusted ports.

This command is not supported on Layer 2 aggregation group member ports. If a Layer 2 Ethernet interface is configured with this command before joining a Layer 2 aggregation group, the command is cleared on the member port after the member ports joins the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 as a PPPoE relay trusted port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] pppoe-relay trust
```

Related commands

pppoe-relay server-information vendor-specific strip

reset pppoe-relay statistics

Use **reset pppoe-relay statistics** to clear packets statistics for the PPPoE relay.

Syntax

reset pppoe-relay statistics

Views

User view

Predefined user roles

network-admin

Examples

Clear packet statistics for the PPPoE relay.

```
<Sysname> reset pppoe-relay statistics
```

Related commands

reset pppoe-relay statistics

New feature: gRPC

Configuring gRPC

About gRPC

gRPC is an open source remote procedure call (RPC) system initially developed at Google. It uses HTTP 2.0 for transport and provides network device configuration and management methods that support multiple programming languages.

gRPC protocol stack layers

Table 20 describes the gRPC protocol stack layers.

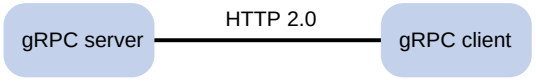
Table 21 gRPC protocol stack layers

Layer	Description
Content layer	Defines the data of the service module. Two peers must notify each other of the data models that they are using.
Protocol buffer encoding layer	Encodes data by using the protocol buffer code format.
gRPC layer	Defines the protocol interaction format for remote procedure calls.
HTTP 2.0 layer	Carries gRPC.
TCP layer	Provides connection-oriented reliable data links.

Network architecture

As shown in Figure 20, the gRPC network uses the client/server model. It uses HTTP 2.0 for packet transport.

Figure 20 gRPC network architecture



The gRPC network uses the following mechanism:

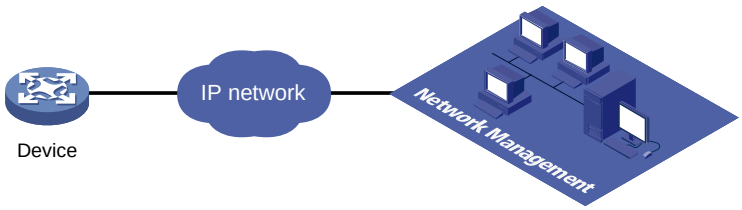
1. The gRPC server listens to connection requests from clients at the gRPC service port.
2. A user runs the gRPC client application to log in to the gRPC server, and uses methods provided in the .proto file to send requests.
3. The gRPC server responds to requests from the gRPC client.

The device can act as the gRPC server or client.

Telemetry technology based on gRPC

Telemetry is a remote data collection technology for monitoring device performance and operating status. HPE telemetry technology uses gRPC to push data from the device to the collectors on the NMSs. As shown in Figure 21, after a gRPC connection is established between the device and NMSs, the NMSs can subscribe to data of modules on the device.

Figure 21 Telemetry technology based on gRPC



Telemetry modes

The device supports the following telemetry modes:

- **Dial-in mode**—The device acts as a gRPC server and the collectors act as gRPC clients. A collector initiates a gRPC connection to the device to subscribe to device data.

  Dial-in mode applies to small networks where collectors need to deploy configurations to devices.
- **Dial-out mode**—The device acts as a gRPC client and the collectors act as gRPC servers. The device initiates a gRPC connection to the collectors and pushes subscribed device data to the collectors.

Dial-out mode applies to larger networks where devices need to push device data to collectors.

Protocols

RFC 7540, *Hypertext Transfer Protocol version 2 (HTTP/2)*

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

gRPC is not supported in FIPS mode.

Configuring the gRPC dial-in mode

gRPC dial-in mode configuration tasks at a glance

To configure the gRPC dial-in mode, perform the following tasks:

1. Configuring the gRPC service
2. Configuring a gRPC user

Configuring the gRPC service

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. (Optional.) Set the gRPC service port number.	**grpc port** *port-number*	By default, the gRPC service port number is 50051.
3. Enable the gRPC service.	**grpc enable**	By default, the gRPC service is disabled.
4. (Optional.) Set the gRPC session idle timeout timer.	**grpc idle-timeout** *minutes*	By default, the gRPC session idle timeout timer is 5 minutes.

Configuring a gRPC user

About gRPC users

For gRPC clients to establish gRPC sessions with the device, you must configure local users for the gRPC clients.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Add a local user with the device management right.	**local-user** *user-name* [**class manage**]	N/A
3. Configure a password for the user.	**password** [{ **hash** | **simple** } *password*]	By default, no password is configured for a local user. A non-password-protected user can pass authentication after providing the correct username and passing attribute checks.
4. Assign user role network-admin to the user.	**authorization-attribute user-role** *user-role*	By default, a local user is assigned the network-operator role.
5. Authorize the user to use the HTTPS service.	**service-type https**	By default, no service types are authorized to a local user.

For more information about the **local-user**, **password**, **authorization-attribute**, and **service-type** commands, see AAA configuration in *Security Command Reference*.

Configuring the gRPC dial-out mode

gRPC dial-out mode configuration tasks at a glance

To configure the gRPC dial-out mode, perform the following tasks:

1. Enabling the gRPC service
2. Configuring sensors
3. Configuring collectors
4. Configuring a subscription

Enabling the gRPC service

Restrictions and guidelines

If the gRPC service fails to be enabled, use the **display tcp** or **display ipv6 tcp** command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again. For more information about the **display tcp** and **display ipv6 tcp** commands, see *Layer 3—IP Services Command Reference*.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the gRPC service.	**grpc enable**	By default, the gRPC service is disabled.

Configuring sensors

About sensors

The device uses sensors to sample data. A sensor path indicates a data source.

Supported data sampling types include:

- **Event-triggered sampling**—Sensors in a sensor group sample data when certain events occur. For sensor paths of this data sampling type, see *NETCONF XML API Event Reference* for the module.
- **Periodic sampling**—Sensors in a sensor group sample data at intervals. For sensor paths of this data sampling type, see the NETCONF XML API references for the module except for *NETCONF XML API Event Reference*.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter telemetry view.	**telemetry**	N/A
3. Create a sensor group and enter sensor group view.	**sensor-group** *group-name*	N/A
4. Specify a sensor path.	**sensor path** *path*	To specify multiple sensor paths, execute this command multiple times.

Configuring collectors

About collectors

Collectors are used to receive sampled data from network devices. For the device to communicate with collectors, you must create a destination group and add collectors to the destination group.

Restrictions and guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter telemetry view.	**telemetry**	N/A
3. Create a destination group and enter destination group view.	**destination-group** *group-name*	N/A
4. Specify a collector.	IPv4: **ipv4-address** *ipv4-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*] IPv6: **ipv6-address** *ipv6-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]	To specify multiple collectors, execute this command multiple times. One collector must have a different address, port, or VPN instance than the other collectors.

Configuring a subscription

About configuring a subscription

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

Procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter telemetry view.	**telemetry**	N/A
3. Create a subscription and enter subscription view.	**subscription** *subscription-name*	N/A
4. (Optional.) Specify the source IP address for packets sent to collectors.	**source-address** { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }	By default, the device uses the primary IPv4 address of the output interface for the route to the collectors as the source address. Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.
5. Specify a sensor group.	**sensor-group** *group-name* [**sample-interval** *interval*]	Specify the **sample-interval** *interval* option for periodic sensor paths and only for periodic sensor paths. If you specify the option for event-triggered sensor paths, the sensor paths do not take effect. If you do not specify the option for periodic sensor paths, the device does not sample or push data.
6. Specify a destination group.	**destination-group** *group-name*	N/A

Display and maintenance commands for gRPC

Execute **display** commands in any view.

Task	Command
Display gRPC information in dial-in mode.	**display grpc**

gRPC configuration examples

These configuration examples describe only CLI configuration tasks on the device. The collectors need to run an extra application.

Example: Configuring the gRPC dial-in mode

Network configuration

As shown in Figure 22, configure the gRPC dial-in mode on the device so the device acts as the gRPC server and the gRPC client can subscribe to LLDP events on the device.

Figure 22 Network diagram

Procedure

1. Assign IP addresses to interfaces on the gRPC server and client and configure routes. Make sure the server and client can reach each other.
2. Configure the device as the gRPC server:

   # Enable the gRPC service.

   ```
   <Device> system-view
   [Device] grpc enable
   ```

   # Create a local user named **test**. Set the password to **test**, and assign user role network-admin and the HTTPS service to the user.

   ```
   [Device] local-user test
   [Device-luser-manage-test] password simple test
   [Device-luser-manage-test] authorization-attribute user-role network-admin
   [Device-luser-manage-test] service-type https
   [Device-luser-manage-test] quit
   ```
3. Configure the gRPC client.
   a. Prepare a PC and install the gRPC environment on the PC. For more information, see the user guide for the gRPC environment.
   b. Obtain the HPE proto definition file and uses the protocol buffer compiler to generate code of a specific language, for example, Java, Python, C/C++, or Go.
   c. Create a client application to call the generated code.
   d. Start the application to log in to the gRPC server.

Verifying the configuration

When an LLDP event occurs on the gRPC server, verify that the gRPC client receives the event.

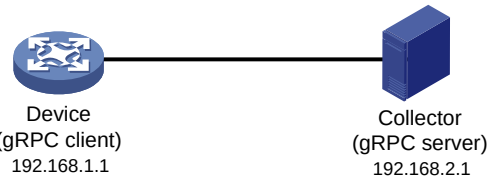
Example: Configuring the gRPC dial-out mode

Network configuration

As shown in Figure 23, the device is connected to a collector. The collector uses port 50050.

Configure gRPC dial-out mode on the device so the device pushes the device capability information of its interface module to the collector at 10-second intervals.

Figure 23 Network diagram



Procedure

Configure IP addresses as required so the device and the collector can reach each other. (Details not shown.)

Enable the gRPC service.

```
<Device> system-view
[Device] grpc enable
```

Create a sensor group named **test**, and add sensor path **ifmgr/devicecapabilities/**.

```
[Device] telemetry
[Device-telemetry] sensor-group test
[Device-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/
[Device-telemetry-sensor-group-test] quit
```

Create a destination group named **collector1**. Specify a collector that uses IPv4 address 192.168.2.1 and port number 50050.

```
[Device-telemetry] destination-group collector1
[Device-telemetry-destination-group-collector1] ipv4-address 192.168.2.1 port 50050
[Device-telemetry-destination-group-collector1] quit
```

Configure a subscription named **A** to bind sensor group **test** with destination group **collector1**. Set the sampling interval to 10 seconds.

```
[Device-telemetry] subscription A
[Device-telemetry-subscription-A] sensor-group test sample-interval 10
[Device-telemetry-subscription-A] destination-group collector1
[Device-telemetry-subscription-A] quit
```

Verifying the configuration

Verify that the collector receives the device capability information of the interface module from the device at 10-second intervals. (Details not shown.)

gRPC dial-in mode commands

display grpc

Use **display grpc** to display gRPC dial-in mode information.

Syntax

display grpc

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display gRPC dial-in mode information.

```
<Sysname> display grpc
gRPC status : enabled.
gRPC port : 50051
gRPC idle-timeout : 3 minutes
Session count: 1.
  Session ID: 1
    User name: test
    Login time:2018-01-05 06:46:43 Idle time : 2 mins 56 s
    Client IP address : 169.254.100.170:40810
    Received RPCs        : 0         Received error RPCs : 0
    Received subscription: 0         Output notifications: 0
```

Table 22 Command output

Field	Description
gRPC status	Status of the gRPC service: • **enabled**—The gRPC service is enabled. • **disabled**—The gRPC service is disabled.
gRPC idle-timeout	Setting for the gRPC session idle timeout timer.
Session count	Number of gRPC sessions.
Idle time	Duration in which the session idle timeout timer will expire. If the value of this field is 0, gRPC sessions will never be timed out.
Received error RPCs	Number of received erroneous gRPC requests.
Received subscription	Number of received gRPC subscription requests.

grpc enable

Use **grpc enable** to enable the gRPC service.

Use **undo grpc enable** to disable the gRPC service.

Syntax

grpc enable

undo grpc enable

Default

The gRPC service is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

If this command fails, use the **display tcp** or **display ipv6 tcp** command to verify whether the gRPC service port number has been used by another feature. If yes, specify a free port as the gRPC service port number and try to enable the gRPC service again.

Examples

Enable the gRPC service.

```
<Sysname> system
[Sysname] grpc enable
```

Related commands

display ipv6 tcp (*Layer 3—IP Services Command Reference*)

display tcp (*Layer 3—IP Services Command Reference*)

grpc port

grpc idle-timeout

Use **grpc idle-timeout** to set the gRPC session idle timeout timer.

Use **undo grpc idle-timeout** to restore the default.

Syntax

grpc idle-timeout *minutes*

undo grpc idle-timeout

Default

The gRPC session idle timeout timer is 5 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the gRPC session idle timeout timer in minutes, in the range of 0 to 30. To disable gRPC sessions from being timed out, set it to 0.

Usage guidelines

If no gRPC packet exchanges occur on the session between a gRPC and the server before the idle timeout timer expires, the device closes the session.

Examples

Set the gRPC session idle timeout timer to 6 minutes.

```
<Sysname> system
[Sysname] grpc idle-timeout 6
```

grpc port

Use **grpc port** to specify the gRPC service port number.

Use **undo grpc port** to restore the default.

Syntax

grpc port *port-number*

undo grpc port

Default

The gRPC service port number is 50051.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the gRPC service port number, in the range of 1 to 65535.

Usage guidelines

You can configure this command only when the gRPC service is disabled.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the gRPC service port number to 50052.

```
<Sysname> system
[Sysname] grpc port 50052
```

Related commands

grpc enable

gRPC dial-out mode commands

destination-group (subscription view)

Use **destination-group** to specify a destination group for a subscription.

Use **undo destination-group** to remove a destination group from a subscription.

Syntax

destination-group *group-name*

undo destination-group *group-name*

Default

A subscription does not have a destination group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

A subscription binds sensor groups to destination groups. Then, the device pushes data from the specified sensors to the collectors.

The specified destination group must have been created by using the **destination-group** command in telemetry view.

You can specify a maximum of three destination groups for a subscription.

Examples

Specify destination group **collector1** for subscription **A**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] destination-group collector1
```

Related commands

destination-group (telemetry view)

destination-group (telemetry view)

Use **destination-group** to create a destination group and enter its view, or enter the view of an existing destination group.

Use **undo destination-group** to delete a destination group.

Syntax

destination-group *group-name*

undo destination-group *group-name*

Default

No destination groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the destination group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

As a best practice, configure a maximum of five destination groups. If you configure too many destination groups, system performance might degrade.

Examples

Create a destination group named **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1]
```

ipv4-address

Use **ipv4-address** to add an IPv4 collector to a destination group.

Use **undo ipv4-address** to remove an IPv4 collector from a destination group.

Syntax

ipv4-address *ipv4-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv4-address *ipv4-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

Default

A destination group does not have IPv4 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IPv4 address of the collector.

port *port-number*: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the collector belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the collector belongs to the public network, do not specify this option.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address, port, or VPN instance than the other collectors.

You can specify a maximum of four collectors for a destination group.

Examples

Add a collector that uses IPv4 address 192.168.21.21 and the default port number to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv4-address 192.168.21.21
```

Related commands

destination-group (telemetry view)

ipv6-address

Use **ipv6-address** to add an IPv6 collector to a destination group.

Use **undo ipv6-address** to remove an IPv6 collector from a destination group.

Syntax

ipv6-address *ipv6-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv6-address *ipv6-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

Default

A destination group does not have IPv6 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IPv6 address of the collector.

port *port-number*: Specifies the listening port of the collector, in the range of 1 to 65535. The default is 50051.

vpn-instance *vpn-instance-name*: Specifies the VPN instance to which the collector belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the collector belongs to the public network, do not specify this option.

Usage guidelines

To add multiple collectors to a destination group, execute this command multiple times.

One collector must have a different address, port, or VPN instance than the other collectors.

You can specify a maximum of four collectors for a destination group.

Examples

Add a collector that uses IPv6 address 1: : 1 and the default port number to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv6-address 1: : 1
```

Related commands

destination-group (telemetry view)

sensor path

Use **sensor path** to configure a sensor path.

Use **undo sensor path** to delete a sensor path.

Syntax

sensor path *path*

undo sensor path *path*

Default

No sensor paths exist.

Views

Sensor group view

Predefined user roles

network-admin

Parameters

path: Specifies a data path. For information about the available paths, enter a question mark (?) in the position of this argument.

Usage guidelines

To configure multiple sensor paths, execute this command multiple times.

The device supports a maximum of 128 sensor paths.

If the device does not support the specified sensor path, the command displays an error message.

Examples

Configure sensor path **ifmgr/devicecapabilities/** for sensor group **test**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test] sensor path ifmgr/devicecapabilities/
```

Related commands

sensor-group (telemetry view)

sensor-group (subscription view)

Use **sensor-group** to specify a sensor group for a subscription.

Use **undo sensor-group** to remove a sensor group from a subscription.

Syntax

sensor-group *group-name* [**sample-interval** *interval*]

undo sensor-group *group-name*

Default

A subscription does not have a sensor group.

Views

Subscription view

Predefined user roles

network-admin

Parameters

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

sample-interval *interval*: Specifies the data sampling interval in seconds. The value range is 1 to 86400.

Usage guidelines

Specify the **sample-interval** *interval* option for periodic sensor paths and only for periodic sensor paths.

- If you specify the option for event-triggered sensor paths, the sensor paths do not take effect.
- If you do not specify the option for periodic sensor paths, the device does not sample or push data.

The specified sensor group must have been created by using the **sensor-group** command in telemetry view.

Examples

Specify sensor group **test** for subscription **A**. Set the data sampling interval to 10 seconds.

```
<Sysname> system-view
[Sysname] telemetry
[Device-telemetry] subscription A
[Device-telemetry-subscription-A] sensor-group test sample-interval 10
```

Related commands

sensor path

sensor-group (telemetry view)

sensor-group (telemetry view)

Use **sensor-group** to create a sensor group and enter its view, or enter the view of an existing sensor group.

Use **undo sensor-group** to delete a sensor group.

Syntax

sensor-group *group-name*

undo sensor-group *group-name*

Default

No sensor groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

group-name: Specifies the sensor group name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of 32 sensor groups.

Examples

Create a sensor group named **test**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] sensor-group test
[Sysname-telemetry-sensor-group-test]
```

source-address

Use **source-address** to specify the source IP address for packets sent to collectors.

Use **undo source-address** to restore the default.

Syntax

source-address { *ipv4-address* | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

undo source-address

Default

The device uses the primary IPv4 address of the output interface for the route to the collectors as the source address.

Views

Subscription view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies an IPv4 address.

interface *interface-type interface-number*: Specifies an interface by its type and number. In the current software version, you must specify a loopback interface. The device will use the interface's primary IPv4 address as the source address. If the interface does not have a primary IPv4 address, the device uses the primary IPv4 address of the output interface for the route to the collectors.

ipv6 *ipv6-address*: Specifies an IPv6 address.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Changing the source IP address for packets sent to collectors causes the device to re-establish the connection to the gRPC server.

Examples

Specify the source IPv4 address of 169.254.1.1 for packets sent to collectors.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A] source-address 169.254.1.1
```

subscription

Use **subscription** to create a subscription and enter its view, or enter the view of an existing subscription.

Use **undo sensor-group** to delete a subscription.

Syntax

subscription *subscription-name*

undo subscription *subscription-name*

Default

No subscription groups exist.

Views

Telemetry view

Predefined user roles

network-admin

Parameters

subscription-name: Specifies the subscription name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

The device supports a maximum of five subscriptions.

Examples

Configure a subscription named **A**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] subscription A
[Sysname-telemetry-subscription-A]
```

Related commands

destination-group (subscription view)

sensor-group (subscription view)

telemetry

Use **telemetry** to enter telemetry view.

Syntax

telemetry

Views

System view

Predefined user roles

network-admin

Usage guidelines

In telemetry view, you can configure telemetry parameters.

Examples

Enter telemetry view.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry]
```

New feature: PBR support for setting default next hops and output interfaces

Setting default next hops or output interfaces

About this task

You can specify a maximum of two default next hops and one default output interface in a PBR.

If a PBR policy contains a default next hop or a default output interface, the device forwards received packets by using the following process:

1. The device uses PBR to forward matching packets.
2. If one of the following events occurs, the device searches for a route (except the default route) in the routing table to forward packets:
   - The packets do not match the PBR policy.
   - The PBR-based forwarding fails.
3. If the forwarding fails, the device uses the default next hop or default output interface defined in PBR to forward packets.
4. If the forwarding fails, the device uses the default route to forward packets.

Setting a default next hop or output interface for IPv4 packets

To set a default next hop or output interface in a PBR policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

2. Enter policy node view.	**policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	N/A
3. Configure actions.	• Set a default next hop: **apply default-next-hop** [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2> • Set a default output interface: **apply default-output-interface** { *interface-type interface-number* [**track** *track-entry-number*] }	By default, no next hops or output interfaces are specified. On a node, you can specify a maximum of two default next hops for backup in one command line or by repeating the command. On a node, you can specify only NULL 0 as the default output interface.

Setting a default next hop or output interface for IPv6 packets

To set a default next hop or output interface in a PBR policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter IPv6 policy node view.	**ipv6 policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*	N/A
3. Configure actions.	• Set default next hops: **apply default-next-hop** [**vpn-instance** *vpn-instance-name*] { *ipv6-address* [**direct**] [**track** *track-entry-number*] }&<1-2> • Set a default output interface: **apply default-output-interface** { *interface-type interface-number* [**track** *track-entry-number*] }	By default, no next hops or output interfaces are specified. On a node, you can specify a maximum of two default next hops for backup in one command line or by repeating the command. On a node, you can specify only NULL 0 as the default output interface.

Command reference

New command: apply default-next-hop

Use **apply default-next-hop** to set default next hops.

Use **undo apply default-next-hop** to remove default next hops.

Syntax

Policy node view:

apply default-next-hop [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>

undo apply default-next-hop [[**vpn-instance** *vpn-instance-name*] *ip-address*&<1-2>]

IPv6 policy node view:

apply default-next-hop [**vpn-instance** *vpn-instance-name*] { *ipv6-address* [**direct**] [**track** *track-entry-number*] }&<1-2>

undo apply default-next-hop [[**vpn-instance** *vpn-instance-name*] *ipv6-address*&<1-2>]

Default

No default next hops are set.

Views

Policy node view

IPv6 policy node 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. The specified VPN instance must already exist.

ip-address: Specifies the IP address of the default next hop. If you do not specify a VPN instance, the default next hop belongs to the public network.

Ipv6-address: Specifies the IPv6 address of the default next hop. If you do not specify a VPN instance, the default next hop belongs to the public network.

direct: Specifies a directly connected default next hop.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

&<1-2>: Indicates that you can specify up to two values for the { *ip-address* [**direct**] [**track** *track-entry-number*] } option.

Usage guidelines

You can specify a maximum of two default next hops for backup in one command line or by executing this command multiple times.

With a default next hop specified, the **undo apply default-next-hop** command removes that default next hop.

Without any default next hops specified, the **undo apply default-next-hop** command removes all default next hops.

Examples

Specify 1.1.1.1 as a directly connected default next hop for matching packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 direct
```

New command: apply default-output-interface

Use **apply default-output-interface** to set a default output interface.

Use **undo apply default-output-interface** to remove the default output interface.

Syntax

apply default-output-interface { *interface-type interface-number* [**track** *track-entry-number*] }

undo apply default-output-interface [{ *interface-type interface-number* }]

Default

No default output interface is set.

Views

Policy node view

IPv6 policy node view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

track *track-entry-number*: Specifies a track entry by its number in the range of 1 to 1024.

Usage guidelines

The default output interface can only be NULL 0.

Examples

Specify NULL 0 as a default output interface for the matching packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-output-interface null 0
```

Modified feature: Specifying the HTTPS redirect listening port number

Feature change description

The default setting for the HTTPS redirect listening port number was changed.

Command changes

Modified command: http-redirect https-port

Syntax

http-redirect https-port *port-number*

undo http-redirect https-port

Views

System view

Change description

Before modification: By default, the HTTPS redirect listening port number is not specified.

After modification: By default, the HTTPS redirect listening port number is 6654.

Modified feature: Configuration archiving

Feature change description

Support for remote archiving was added. Remote archiving saves the running configuration to a remote SCP server.

Command changes

New command: archive configuration server

Use **archive configuration server** to configure the parameters for archiving the running configuration to a remote SCP server.

Use **undo archive configuration server** to restore the default.

Syntax

archive configuration server scp { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **filename-prefix** *filename-prefix*

undo archive configuration server

Default

No parameters are set for archiving the running configuration to a remote SCP server.

Views

System view

Predefined user roles

network-admin

Parameters

scp: Specifies a remote SCP server.

ipv4-address: Specifies the SCP server by its IPv4 address.

ipv6 *ipv6-address*: Specifies the SCP server by its IPv6 address.

port *port-number*: Specifies the TCP port number of the SCP server, in the range of 0 to 65535. The default TCP port number is 22.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the SCP server is on the public network, do not specify this option.

directory *directory*: Specifies the archive directory, a case-insensitive string. If you do not specify this option, the archive directory is the root directory of the SCP server.

filename-prefix *filename-prefix*: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

IMPORTANT:

In FIPS mode, the device does not support archiving the running configuration to a remote SCP server.

Before archiving the running configuration to a remote SCP server, you must perform the following tasks:

- Use this command to specify a configuration archive directory and a name prefix on the remote SCP server.
- Use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

To manually archive the running configuration, use the **archive configuration** command. To periodically archive the running configuration, use the **archive configuration interval** command.

On the specified remote SCP server, configuration archives are named in the format of *filename-prefix_YYYYMMDD_HHMMSS***.cfg** (for example, **archive_20170526_203430.cfg**).

Local archiving (the **archive configuration location** command) and remote archiving (the **archive configuration server** command) are mutually exclusive. You cannot use the two features at the same time.

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the **archive configuration max** command.

The **undo archive configuration server** command removes the configuration archive directory and file name prefix settings, but it does not delete the configuration archives saved on the server. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default setting for the **archive configuration interval** command.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **archive/** on the SCP server at 192.168.1.1 and set the archive file name prefix as **my_archive**.

```
<Sysname> system-view
[Sysname] archive configuration server scp 192.168.1.1 port 22 directory /archive/
filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration server password

archive configuration server user

display archive configuration

New command: archive configuration server password

Use **archive configuration server password** to configure the password for accessing the SCP server that saves the configuration archives.

Use **undo archive configuration server password** to restore the default.

Syntax

archive configuration server password { **cipher** | **simple** } *string*

undo archive configuration server password

Default

No password is configured for accessing the SCP server that saves the configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

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.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

Set the password to **admin** in plaintext form for accessing the SCP server that saves the configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server password simple admin
```

Related commands

archive configuration server

archive configuration server user

display archive configuration

New command: archive configuration server user

Use **archive configuration server user** to configure the username for accessing the SCP server that saves the configuration archives.

Use **undo archive configuration server user** to restore the default.

Syntax

archive configuration server user *user-name*

undo archive configuration server user

Default

No username is configured for accessing the SCP server that saves the configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Examples

Set the username to **admin** for accessing the SCP server that saves the configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server user admin
```

Related commands

archive configuration server

archive configuration server password

display archive configuration

Modified command: display archive configuration

Syntax

display archive configuration

Views

Any view

Change description

The command output has the following changes:

- The **Username** field was added to display information about the configuration archives saved on a remote SCP server. This field displays the username used for accessing to the remote SCP server.
- The **Saved archive files**, **TimeStamp**, and **FileName** fields were changed to **Archive history**, **Timestamp**, and **Filename**, respectively, with their purposes unchanged.
- The exclamation mark (!) was added before an archive file number to indicate that the remote archiving attempt has failed.

The following examples show samples of the command output before modification and after modification:

Before modification:

Display information about the configuration archives.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Saved archive files:
  No. TimeStamp                  FileName
  1   Wed Dec 15 14:20:18 2010   my_archive_1.cfg
  2   Wed Dec 15 14:33:10 2010   my_archive_2.cfg
# 3   Wed Dec 15 14:49:37 2010   my_archive_3.cfg
‘#’ indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Table 1 Command output

Field	Description
Location	Absolute path of the directory for saving running-configuration archives.
Filename prefix	File name prefix for configuration archives.
Archive interval in minutes	Interval (in minutes) for the system to automatically archive the running configuration. If automatic configuration saving is disabled, this field is not available.
Maximum number of archive files	Maximum number of configuration archives that can be saved.
Saved archive files	History configuration archive information.
No.	Number of a configuration archive.
TimeStamp	Time when the configuration archive was created.
FileName	Configuration archive file name, not including the file path.

After modification:

Display information about the configuration archives. The sample output was created based on local archiving.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Archive history:
  No.  Timestamp               Filename
  1    Aug 05 2007 20:24:54    my_archive_1.cfg
  2    Aug 05 2007 20:34:54    my_archive_2.cfg
# 3    Aug 05 2007 20:44:54    my_archive_3.cfg
The pound sign (#) indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Display information about the configuration archives. The sample output was created based on remote archiving.

```
<Sysname> display archive configuration
Username: test
Location: scp://192.168.21.21:22/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Archive history:
 No.   Timestamp                 Filename
 1     Wed Dec 15 14:20:18 2010  my_archive_20170509_142018.cfg
!2     Wed Dec 15 14:33:10 2010  my_archive_20170509_143018.cfg
#!3    Wed Dec 15 14:49:37 2010  my_archive_20170509_144018.cfg
The exclamation mark (!) indicates that the remote archiving attempt failed.
The pound sign (#) indicates the most recent archive file.
```

Table 2 Command output

Field	Description
Username	Username for logging in to the SCP server that saves the configuration archives.
Location	Absolute path of the directory for saving running-configuration archives.
Filename prefix	File name prefix for configuration archives.
Archive interval in minutes	Interval (in minutes) for the system to automatically archive the running configuration. If automatic configuration saving is disabled, this field is not available.
Maximum number of archive files	Maximum number of configuration archives that can be saved. This field is available only for local archiving.
Archive history	History configuration archive information.
No.	Number of a configuration archive.
Timestamp	Time when the configuration archive was created.
Filename	Configuration archive file name, not including the file path.

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

archive configuration server user

Modified feature: Specifying startup images and completing the upgrade

Feature change description

In this version, you can specify patch image files when performing a software upgrade.

Command changes

Modified command: boot-loader file

Old syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

New syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

Views

User view

Change description

The **patch** *filename* option was added.

patch *filename*&<1-16>: Specifies a space-separated list of up to 16 patch image files. You can specify only non-incremental patch image files. Because the boot, system, and feature images each can have one non-incremental patch image file, the device can use a maximum of 16 non-incremental patch image files.

Modified feature: ISSU

Feature change description

The **patch** *filename*&<1-16> option was added to the **display version comp-matrix** and **issu load** commands to display patch image information and install patch images.

Command changes

Modified command: display version comp-matrix file

Old syntax

display version comp-matrix

display version comp-matrix file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } *

display version comp-matrix file ipe *ipe-filename*

New syntax

display version comp-matrix file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-16> } *

display version comp-matrix file ipe *ipe-filename* [**patch** *filename*&<1-16>]

Views

Any view

Change description

patch: Specifies a space-separated list of up to 16 patch image files.

Modified command: issu load

Old syntax

issu load file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number*&<1-9>[**reboot**]

issu load file ipe *ipe-filename* **slot** *slot-number*&<1-9> [**reboot**]

New syntax

issu load file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-16> } *** slot** *slot-number*&<1-9> [**reboot**]

issu load file ipe *ipe-filename* [**patch** *filename*&<1-16>] **slot** *slot-number*&<1-9> [**reboot**]

Views

User view

Change description

patch: Specifies a space-separated list of up to 16 patch image files. You can specify both incremental and non-incremental patch image files. For information about incremental and non-incremental patch images, see software upgrade in *Fundamentals Configuration Guide*.

Modified feature: Memory depletion alarming

Feature change description

You can set memory depletion alarm resending intervals.

Command changes

New command: monitor resend memory-threshold

Use **monitor resend memory-threshold** to set memory depletion alarm resending intervals.

Use **undo monitor resend memory-threshold** to restore default settings.

Syntax

monitor resend memory-threshold { **critical-interval** *critical-interval* | **early-warning-interval** *early-warning-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend memory-threshold [**critical-interval** | **early-warning-interval** | **minor-interval** | **severe-interval**] * [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

- Early warning resending interval: 1 hour.
- Minor alarm resending interval: 12 hours.
- Severe alarm resending interval: 3 hours.
- Critical alarm resending interval: 1 hour.

Views

System view

Predefined user roles

network-admin

Parameters

critical-interval *critical-interval*: Specifies the critical alarm resending interval in hours, in the range of 1 to 48.

early-warning-interval *early-warning-interval*: Specifies the early warning resending interval in hours, in the range of 1 to 48.

minor-interval *minor-interval*: Specifies the minor alarm resending interval in hours, in the range of 1 to 48.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in hours, in the range of 1 to 48.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples the amount of free memory space periodically and compares the sample with free-memory thresholds. If the sample decreases to or below a threshold, the device enters a memory depletion alarm state and sends an alarm.

In critical alarm state, the device sends critical alarm notifications periodically until the critical alarm is removed.

In a lower alarm state, the device sends notifications for the alarm state periodically until it enters a higher alarm state or the current alarm is removed.

You can use this command to change the alarm resending intervals.

If you do not specify any memory depletion alarm resending intervals, the **undo monitor resend memory-threshold** command restores default settings for all memory depletion alarm resending intervals.

Examples

Set the minor memory depletion alarm resending interval to 12 hours for CPU 0 in slot 1.

```
<Sysname> system-view
[Sysname] monitor resend memory-threshold minor-interval 12 slot 1 cpu 0
```

Modified feature: CPU usage monitoring

Feature change description

You can monitor CPU usage in more granularity and set CPU usage alarm resending intervals.

Command changes

Modified command: monitor cpu-usage threshold

Old syntax

monitor cpu-usage threshold *cpu-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

New syntax

monitor cpu-usage threshold *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage threshold minor-threshold recovery-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

System view

Change description

Before modification: Only one CPU usage alarm threshold is supported.

After modification: You can set the severe CPU usage alarm threshold, minor CPU usage alarm threshold, and CPU usage recovery threshold.

severe-threshold: Specifies the severe CPU usage alarm threshold in percentage. The value range for this argument is 2 to 100.

minor-threshold *minor-threshold*: Specifies the minor CPU usage alarm threshold in percentage. The value range for this argument is 1 to the severe CPU usage alarm threshold minus 1.

recovery-threshold *recovery-threshold*: Specifies the CPU usage recovery threshold in percentage. The value range for this argument is 0 to the minor CPU usage alarm threshold minus 1.

Modified command: display cpu-usage

Old syntax

display cpu-usage [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

New syntax

display cpu-usage [**summary**] [**slot** *slot-number* [**cpu** *cpu-number* [**core** { *core-number*| **all** }]]]

display cpu-usage [**control-plane** | **data-plane**] [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]

Views

Any view

Change description

The **control-plane**, **data-plane**, and **core** { *core-number* | **all** } options were added.

control-plane: Displays CPU usage statistics for the control plane. If you do not specify this keyword or the **data-plane** keyword, the command displays the total CPU usage statistics.

data-plane: Displays CPU usage statistics for the data plane. If you do not specify this keyword or the **control-plane** keyword, the command displays the total CPU usage statistics.

core *core-number*: Specifies a CPU core by its number.

core all: Specifies all CPU cores.

New command: monitor cpu-usage threshold

Use **monitor resend cpu-usage** to set CPU usage alarm resending intervals.

Use **undo monitor resend cpu-usage** to restore default settings.

Syntax

monitor resend cpu-usage { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend cpu-usage [**minor-interval** | **severe-interval**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The minor alarm resending interval is 300 seconds. The severe alarm resending interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

minor-interval *minor-interval*: Specifies the minor alarm resending interval in seconds, a multiple of 5 in the range of 10 to 3600.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in seconds, a multiple of 5 in the range of 10 to 3600.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage periodically and compares the sample with the CPU usage threshold. If the sample increases above an alarm threshold, the CPU usage enters an alarm state and the device sends an alarm.

While the CPU usage is in minor alarm state, the device sends minor alarms periodically until the CPU usage increases above the severe threshold or the minor alarm is removed.

While the CPU usage is in severe alarm state, the device sends severe alarms periodically until the severe alarm is removed.

You can use this command to change CPU usage alarm resending intervals.

If you do not specify the **minor-interval** or **severe-interval** keyword, the **undo monitor resend cpu-usage** command restores default settings for both the minor and severe alarm resending intervals.

Examples

Set the CPU usage minor alarm resending interval to 60 seconds for CPU 0 in slot 1.

```
<Sysname> system-view
[Sysname] monitor resend cpu-usage minor-interval 60 slot 1 cpu 0
```

Modified feature: Device power supply monitoring

Feature change description

You can display detailed power supply information about the device.

Command changes

Modified command: display power

Old syntax

display power [**slot** *slot-number* [*power-id*]]

New syntax

display power [**slot** *slot-number* [*power-id* | **verbose**]]

Views

Any view

Change description

The **verbose** keyword was added.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Modified feature: Creating a BFD session for detecting the local interface state

Feature change description

In this version, new interfaces types that can be detected were added.

Command changes

Modified command: bfd detect-interface

Syntax

bfd detect-interface source-ip *ip-address*

undo bfd detect-interface

Views

Interface view

Change description

Before modification, you can associate the state of the following interfaces with BFD:

- Layer 3 Ethernet interfaces.
- Member ports in a Layer 3 aggregation group.
- Layer 3 Ethernet subinterfaces.
- VLAN interfaces.

After modification, you can associate the state of the following interfaces with BFD:

- Layer 2 Ethernet interfaces.
- Member ports in a Layer 2 aggregation group.
- Layer 3 Ethernet interfaces.
- Member ports in a Layer 3 aggregation group.
- Layer 3 Ethernet subinterfaces.
- VLAN interfaces.
- Layer 2 aggregate interfaces.
- Layer 3 aggregate interfaces.

Modified feature: Setting the DHCP server response timeout time

Feature change description

The value range for the DHCP server response timeout time was changed.

Command reference

Modified command: dhcp relay dhcp-server timeout

Use **dhcp relay dhcp-server timeout** to set the DHCP server response timeout time for DHCP server switchover.

Use **undo dhcp relay dhcp-server timeout** to restore the default.

Syntax

dhcp relay dhcp-server timeout *time*

undo dhcp relay dhcp-server timeout

Views

Interface view

Change description

Before modification: The value range for the *time* argument is 30 to 65535 seconds.

After modification: The value range for the *time* argument is 1 to 65535 seconds.

Modified command: dhcp-server timeout

Use **dhcp-server timeout** to set the DHCP server response timeout time for DHCP server switchover.

Use **undo dhcp-server timeout** to restore the default.

Syntax

dhcp-server timeout *time*

undo dhcp-server timeout

Views

DHCP address pool view

Change description

Before modification: The value range for the *time* argument is 30 to 65535 seconds.

After modification: The value range for the *time* argument is 1 to 65535 seconds.

Modified feature: Displaying ND snooping entries

Feature change description

Commands for displaying information about ND snooping entries were changed.

Command reference

New command: display ipv6 nd snooping vlan

Use **display ipv6 nd snooping vlan** to display ND snooping entries in the specified VLAN

Syntax

display ipv6 nd snooping vlan [[*vlan-id* | **interface** *interface-type interface-number*] [**global** | **link-local**] | *ipv6-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Displays ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

interface *interface-type interface-number*: Displays ND snooping entries for the specified interface in a VLAN. The *interface-type interface-number* argument specifies an interface by its type and number.

global: Displays ND snooping entries for global unicast addresses in the VLAN.

link-local: Displays ND snooping entries for link-local addresses in the VLAN.

ipv6-address: Displays the ND snooping entry for the specified IPv6 address.

verbose: Displays detailed information about ND snooping entries in the VLAN. If you do not specify the keyword, this command displays brief information about ND snooping entries.

Usage guidelines

If you do not specify any parameters, this command displays all ND snooping entries.

Examples

Display brief information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1

IPv6 address              MAC address     VID  Interface     Status       Age

1::2                       0000-1234-0c01  1    GE1/0/2        VALID        57
```

Display detailed information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1 verbose

IPv6 address: 1::2

MAC address: 0000-1234-0c01

Interface: GE1/0/2

First VLAN ID: 1   Second VLAN ID: N/A

Status: VALID   Age: 57
```

Table 23 Command output

Field	Description
IPv6 address	IPv6 address in the ND snooping entry.
MAC address	MAC address in the ND snooping entry.
VID	ID of the VLAN to which the ND snooping entry belongs.
First VLAN ID	ID of the SVLAN to which the ND snooping entry belongs.
Second VLAN ID	ID of the CVLAN to which the ND snooping entry belongs. If no CVLAN is configured, this field displays **N/A**. For more information about the SVLAN and CVLAN, see QinQ in *Layer 2—LAN Switching Configuration Guide*.
Interface	Input interface in the ND snooping entry.

Status	Status of the ND snooping entry:
	• **TENTATIVE**—The entry is ineffective.
	• **VALID**—The entry is effective.
	• **TESTING_TPLT**—The entry is being tested by DAD. The device performs DAD for the entry in the following situations:
	  ○ The entry ages out.
	  ○ An ND trusted interface in the VLAN receives an ND message from the IPv6 address in the entry.
	• **TESTING_VP**—The entry is being tested by DAD. The device performs DAD when an ND untrusted interface in the VLAN receives an ND message from the IPv6 address in the entry.

Age	For an ND snooping entry in VALID status, this field displays its remaining aging time in seconds. For an ND snooping entry in other status, this field displays a pound sign (#).

Related commands

ipv6 nd snooping enable global

ipv6 nd snooping enable link-local

New command: display ipv6 nd snooping count vlan

Use **display ipv6 nd snooping count vlan** to display the number of IPv6 ND snooping entries for VLANs.

Syntax

display ipv6 nd snooping count vlan [**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, this command displays the total number of ND snooping entries in all VLANs.

Examples

Display the total number of IPv6 ND snooping entries in all VLANs.

```
<Sysname> display ipv6 nd snooping count vlan

Total entries for VLANs: 5
```

Display the total number of IPv6 ND snooping entries on GigabitEthernet 1/0/1.

```
<Sysname> display ipv6 nd snooping count vlan interface gigabitethernet 1/0/1

Total entries on interface: 2
```

Table 24 Command output

Field	Description
Total entries for VLANs	Total number of ND snooping entries in all VLANs.
Total entries on interface	Total number of ND snooping entries on the interface.

Related commands

ipv6 nd snooping enable global

ipv6 nd snooping enable link-local

reset ipv6 nd snooping vlan

New command: reset ipv6 nd snooping vlan

Use **reset ipv6 nd snooping vlan** to clear ND snooping entries in VLANs.

Syntax

reset ipv6 nd snooping vlan { [*vlan-id*] [**global | link-local**] **|** *vlan-id ipv6-address* }

Views

User view

Predefined user roles

network-admin

Parameters

vlan-id: Clears ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

global: Clears ND snooping entries for global unicast addresses.

link-local: Clears ND snooping entries for link-local addresses.

vlan-id ipv6-address: Clears the ND snooping entry of the specified IPv6 address in the specified VLAN. The value range for the VLAN ID is 1 to 4094.

Usage guidelines

If you do not specify any parameters, this command clears ND snooping entries in all VLANs.

Examples

Clear ND snooping entries in all VLANs.

```
<Sysname> reset ipv6 nd snooping vlan
```

Related commands

display ipv6 nd snooping count vlan

display ipv6 nd snooping vlan

Removed command: display ipv6 nd snooping count

Use **display ipv6 nd snooping count** to display the number of ND snooping entries.

Syntax

display ipv6 nd snooping count [**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.

Examples

Display the number of ND snooping entries on the device.

```
<Sysname> display ipv6 nd snooping count
Total number of entries: 5
```

Display the number of ND snooping entries on GigabitEthernet1/0/1.

```
<Sysname> display ipv6 nd snooping count interface gigabitethernet 1/0/1
Total number of entries on interface: 2
```

Table 25 Command output

Field	Description
Total number of entries	Total number of ND Snooping entries on the device.
Total number of entries on interface: *number*	Total number of ND Snooping entries on an interface.

Removed command: display ipv6 nd snooping

Use **display ipv6 nd snooping** to display information about ND snooping entries.

Syntax

display ipv6 nd snooping [[[**vlan** *vlan-id* | **interface** *interface-type interface-number*] [**global** | **link-local**]] **|** *ipv6-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vlan *vlan-id*: Displays ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

interface *interface-type interface-number*: Displays ND snooping entries for the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number.

ipv6-address: Displays the ND snooping entry for the specified IPv6 address.

global: Displays ND snooping entries for global unicast addresses in the VLAN.

link-local: Displays ND snooping entries for link-local addresses in the VLAN.

verbose: Displays detailed information about ND snooping entries in the VLAN. If you do not specify the keyword, this command displays brief information about ND snooping entries.

Examples

Display brief information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1
IPv6 address              MAC address     VID  Interface     Status       Age
1::2                       0000-1234-0c01  1    GE1/0/2        VALID        57
```

Display detailed information about IPv6 ND snooping entries for VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1 verbose
IPv6 address: 1::2
MAC address: 0000-1234-0c01
Interface: GE1/0/2
First VLAN ID: 1   Second VLAN ID: N/A
Status: VALID   Age: 57
```

Table 26 Command output

Field	Description
IPv6 address	IPv6 address in the ND snooping entry.

Field	Description
MAC address	MAC address in the ND snooping entry.
VID	ID of the VLAN to which the ND snooping entry belongs.
First VLAN ID	ID of the SVLAN to which the ND snooping entry belongs.
Second VLAN ID	ID of the CVLAN to which the ND snooping entry belongs. If no CVLAN is configured, this field displays **N/A**. For more information about the SVLAN and CVLAN, see QinQ in *Layer 2—LAN Switching Configuration Guide*.
Interface	Input interface in the ND snooping entry.

Status	Status of the ND snooping entry:
	• **TENTATIVE**—The entry is ineffective.
	• **VALID**—The entry is effective.
	• **TESTING_TPLT**—The entry is being tested by DAD. The device performs DAD for the entry in the following situations:
	  ○ The entry ages out.
	  ○ An ND trusted interface in the VLAN receives an ND message from the IPv6 address in the entry.
	• **TESTING_VP**—The entry is being tested by DAD. The device performs DAD when an ND untrusted interface in the VLAN receives an ND message from the IPv6 address in the entry.

Age	For an ND snooping entry in VALID status, this field displays its remaining aging time in seconds. For an ND snooping entry in other status, this field displays a pound sign (#).

Removed command: reset ipv6 nd snooping

Use **reset ipv6 nd snooping** to clear ND snooping entries.

Syntax

reset ipv6 nd snooping [[**vlan** *vlan-id*] [**global** | **link-local**] | **vlan** *vlan-id ipv6-address*]

Views

User view

Predefined user roles

network-admin

Parameters

vlan-id: Clears ND snooping entries for the specified VLAN. The value range for the VLAN ID is 1 to 4094.

global: Clears ND snooping entries for global unicast addresses.

link-local: Clears ND snooping entries for link-local addresses.

vlan *vlan-id ipv6-address*: Clears the ND snooping entry of the specified IPv6 address in the specified VLAN. The value range for the VLAN ID is 1 to 4094.

Examples

Clear ND snooping entries on the device.

```
<Sysname> reset ipv6 nd snooping
```

Modified feature: Port security intrusion protection

Feature change description

The **port-security timer blockmac** *time-value* command was added to set the block timer for blocked MAC addresses.

The device adds the source MAC addresses of illegal frames to the blocked MAC address list if the intrusion protection action is blocking MAC addresses.

The block timer sets the amount of time that a MAC address must remain in the blocked MAC address list before it is unblocked.

Command changes

New command: port-security timer blockmac

Use **port-security timer blockmac** to set the block timer for MAC addresses in the blocked MAC address list.

Use **undo port-security timer blockmac** to restore the default.

Syntax

port-security timer blockmac *time-value*

undo port-security timer blockmac

Default

The block timer for blocked MAC addresses is 180 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Sets a timer value in the range of 1 to 3600 seconds.

Usage guidelines

Use the block timer in conjunction with the intrusion protection action that blocks the source MAC addresses of illegal frames.

The block timer sets the amount of time that a MAC address must remain in the blocked MAC address list before it is unblocked.

Examples

Configure the intrusion protection action on GigabitEthernet 1/0/1 as blocking source MAC addresses of illegal frames, and set the block timer to 60 seconds.

```
<Sysname> system-view
[Sysname] port-security timer blockmac 60
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

Related commands

display port-security

port-security intrusion-mode

Modified command: display port-security

Syntax

display port-security [**interface** *interface-type interface-number*]

Views

Any view

Change description

The **Blockmac timeout** field was added to the command output to display the block timer (in seconds) for MAC addresses in the blocked MAC address list.

Modified feature: Managing passwords for device management users

Feature change description

From this release, the password management changes for device management users.

Command changes

Modified command: password (device management user view)

Syntax

In non-FIPS mode:

password [{ **hash** | **simple** } *string*]

undo password

In FIPS mode:

password

Views

Device management user view

Change description

Before modification: The password specified in plaintext form will be stored in encrypted form.

After modification: The password specified in plaintext form will be stored in hashed form.

When global password control is enabled, the device handles passwords of device management users as follows:

- All passwords in the history records are saved in hashed form.
- If a user changes its own password in plaintext form, the system requests the user to enter the current plaintext password. The new password must be different from all passwords in the history records and the current password. In addition, the new password must have a minimum of four characters different from the current password.
- If a user changes the password for another user in plaintext form, the new password must be different from the latter user's all passwords in the history records and current password.

- If a user deletes its own password, the system requests the user to enter the current plaintext password.
- Except the above listed situations, the system does not request a user to enter the current plaintext password or compare the new password with the history passwords and the current password.

Modified command: password-control { aging | composition | history | length } enable

Syntax

password-control { **aging** | **composition** | **history** | **length** } **enable**

undo password-control { **aging** | **composition** | **history** | **length** } **enable**

Views

System view

Change description

If the global password control feature is enabled but the minimum password length restriction feature is disabled, the following rules apply for device management users:

- Before modification:
  - In non-FIPS mode, a password must contain a minimum of 4 characters and a minimum of 4 characters must be different.
  - In FIPS mode, a password must contain a minimum of 15 characters and a minimum of 4 characters must be different.
- After modification: A password must contain a minimum of 4 characters in non-FIPS mode and a minimum of 15 characters in FIPS mode. The password composition requirements depend on the password composition policy set for the device management users.

Modified feature: Destination-based portal-free rules

Feature change description

In this version, the requirements for the host name in a destination-based portal-free rule were changed.

Command changes

Modified command: portal free-rule destination

Syntax

portal free-rule *rule-number* **destination** *host-name*

undo portal free-rule { *rule-number* | **all** }

Views

System view

Change description

The requirements for the *host-name* argument were changed.

Before modification: The host name is a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*). The host name string cannot be **ip** or **ipv6**.

After modification: The host name is a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*). The host name string cannot be **i**, **ip**, **ipv**, or **ipv6**.

Modified feature: Displaying IPv4SG bindings

Feature change description

In this version, the **arp-snooping** keyword in the **display ip source binding** command and the **nd-snooping** keyword in the **display ipv6 source binding** command were changed to **arp-snooping-vlan** and **nd-snooping-vlan**, respectively.

Command changes

Modified command: display ip source binding

Old syntax

display ip source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**arp-snooping** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

New syntax

display ip source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**arp-snooping-vlan** | **dhcp-relay** | **dhcp-server** | **dhcp-snooping** | **dot1x**]] [**ip-address** *ip-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any views

Change description

The **arp-snooping** keyword was changed to **arp-snooping-vlan**.

arp-snooping-vlan: Specifies IPv4SG bindings generated based on ARP snooping for VLANs.

Modified command: display ipv6 source binding

Old syntax

display ipv6 source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcpv6-relay** | **dhcpv6-snooping** | **dot1x** | **nd-snooping**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

New syntax

display ipv6 source binding [**static** | [**vpn-instance** *vpn-instance-name*] [**dhcpv6-relay** | **dhcpv6-snooping** | **dot1x** | **nd-snooping-vlan**]] [**ip-address** *ipv6-address*] [**mac-address** *mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-number*] [**slot** *slot-number*]

Views

Any views

Change description

The **nd-snooping** keyword was changed to **nd-snooping-vlan**.

nd-snooping-vlan: Specifies IPv6SG bindings generated based on ARP snooping for VLANs.

Modified feature: Displaying and maintaining ARP attack detection

Feature change description

The commands for displaying and maintaining ARP attack detection were changed.

Command changes

New command: display arp detection statistics attack-source

Use **display arp detection statistics attack-source** to display statistics for ARP attack sources.

Syntax

display arp detection statistics attack-source slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack source statistics for the master device.

Examples

Display statistics for ARP attack sources on slot 1.

```
<Sysname> display arp detection statistics attack-source slot 1
Interface              VLAN  MAC address    IP address      Number     Time
GE1/0/1                1     0005-0001-0001 10.1.1.14       24         17:09:56
03-27-2017
```

Table 27 Command output

Field	Description
Interface	Receiving interface of ARP attack packets.
VLAN	VLAN to which ARP attack packets belong.
MAC address	Sender MAC address in ARP attack packets.
IP address	Sender IP address in ARP attack packets.
Number	Number of ARP attack packets dropped by ARP attack detection.
Time	The most recent time when ARP attack detection dropped an ARP attack packet.

Related commands

arp detection enable

New command: display arp detection statistics packet-drop

Use **display arp detection statistics packet-drop** to display statistics for packets dropped by ARP attack detection.

Syntax

display arp detection statistics packet-drop [**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, this command displays dropped packet statistics for all interfaces.

Usage guidelines

This command displays numbers of packets discarded by user validity check and ARP packet validity check on interfaces.

Examples

Display statistics for packets dropped by ARP attack detection.

```
<Sysname> display arp detection statistics packet-drop
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
GE1/0/3(T)                  0         0         0         0
GE1/0/4(U)                  0         0         30        0
GE1/0/5-srv1(U)             0         10        20        0
GE1/0/5-srv2(T)             10        0         20        22
```

Table 28 Command output

Field	Description
State	State of an interface: • **U**—ARP untrusted interface. • **T**—ARP trusted interface.
Interface(State)	Inbound interface of ARP packets. **State** specifies the port state, **trusted** or **untrusted**.
IP	Number of ARP packets discarded due to invalid sender and target IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.

Field	Description
Inspect	Number of ARP packets that failed to pass user validity check.

Related commands

reset arp detection statistics packet-drop

New command: reset arp detection statistics attack-source

Use **reset arp detection statistics attack-source** to clear statistics for ARP attack sources.

Syntax

reset arp detection statistics attack-source [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command clears ARP attack source statistics for the master device.

Examples

Clear statistics for ARP attack sources.

```
<Sysname> reset arp detection statistics attack-source
```

Related commands

arp detection enable

display arp detection statistics attack-source

New command: reset arp detection statistics packet-drop

Use **reset arp detection statistics packet-drop** to clear statistics for packets dropped by ARP attack detection.

Syntax

reset arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears dropped packet statistics for all interfaces.

Examples

Clear statistics for packets dropped by ARP attack detection.

```
<Sysname> reset arp detection statistics packet-drop
```

Related commands

display arp detection statistics packet-drop

Removed command: display arp detection statistics

Syntax

display arp detection statistics [**interface** *interface-type interface-number*]

Views

Any views

Removed command: reset arp detection statistics

Syntax

reset arp detection statistics [**interface** *interface-type interface-number*]

Views

User view

Modified feature: Displaying and clearing log information about purged or refreshed LSPs

Feature change description

Support for displaying and clearing log information about purged or refreshed LSPs was added.

Command changes

Modified command: display isis event-log lsp

Old syntax

display isis event-log lsp [**level-1** | **level-2**] * [*process-id*]

New syntax

display isis event-log lsp { **purged** | **refreshed** } [**level-1** | **level-2**] * [*process-id*]

Views

Any view

Change description

Before modification: The **purged** and **refreshed** keywords are not supported.

After modification: The **purged** and **refreshed** keywords are supported. You can specify the **purged** keyword to display log information about purged LSPs or specify the **refreshed** keyword to display log information about refreshed LSPs, including generated and received LSPs.

Modified command: reset isis event-log lsp

Old syntax

reset isis event-log lsp [*process-id*]

New syntax

display isis event-log lsp { **purged** | **refreshed** } [**level-1** | **level-2**] * [*process-id*]

Views

User view

Change description

Before modification: The **purged** and **refreshed** keywords are not supported.

After modification: The **purged** and **refreshed** keywords are supported. You can specify the **purged** keyword to clear log information about purged LSPs or specify the **refreshed** keyword to clear log information about refreshed LSPs, including generated and received LSPs.

Modified feature: Displaying PIM routing entries

Feature change description

The device supports displaying PIM routing entries that contain the **2mvpn** flag.

Command reference

Modified command: display pim routing-table

Syntax

display pim [**vpn-instance** *vpn-instance-name*] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **flags** *flag-value* | **fsm** | **incoming-interface** *interface-type interface-number* | **mode** *mode-type* | **outgoing-interface** { **exclude** | **include** | **match** } *interface-type interface-number* | **proxy**] *

Views

Any view

Change description

The **2mvpn** flag value was added to the **flags** *flag-value* option.

flags *flag-value*: Specifies a flag. If you do not specify a flag, this command displays PIM routing entries that contain all flags.

2mvpn: Specifies PIM routing entries that have been advertised to MVPN.

Modified feature: Setting the maximum size of a join or prune message

Feature change description

The default maximum size of a join or prune message was changed.

Command reference

Modified command: jp-pkt-size

Syntax

jp-pkt-size *size*

undo jp-pkt-size

Views

PIM view

IPv6 PIM view

Change description

Before modification: The default maximum size of a join or prune message is 8100 bytes.

After modification: The default maximum size of a join or prune message is 1200 bytes.

Modified feature: Physical state change suppression on an Ethernet interface

Feature change description

The **link-delay** syntax was changed.

Command changes

Modified command: link-delay

Old syntax

link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

undo link-delay [**msec**] *delay-time* [**mode** { **up** | **updown** }]

New syntax

link-delay { **down** | **up** } [**msec**] *delay-time*

undo link-delay { **down** | **up** }

Views

Ethernet interface view

Change description

The **down** keyword was added. Specifying the **down** keyword in the new syntax equals not specifying the **mode** keyword in the old syntax.

- **down**: Suppresses link-down events.

The **mode updown** keyword was removed:

- **mode updown**: Suppresses both the link-up and link-down events.

To implement the effect of specifying the **mode updown** keyword in the old syntax, configure link-up event suppression and link-down event suppression separately by using the new syntax.

Modified feature: Configuring a link aggregation load sharing hash seed

Feature change description

The value range for the hash seed was modified to 0 to FFFFFFFF.

Command changes

Modified command: link-aggregation global load-sharing seed

Syntax

link-aggregation global load-sharing seed *seed-number*

Views

System view

Change description

Before modification: The value range for the *seed-number* argument is 1 to FFFFFFFF.

After modification: The value range for the *seed-number* argument is 0 to FFFFFFFF.

Modified feature: MAC-VLAN entries

Feature change description

A keyword of the **mac-vlan mac-address** command was modified.

Command changes

Modified command: mac-vlan mac-address

Old syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1q** *priority*]

New syntax

mac-vlan mac-address *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**dot1p** *priority*]

Views

System view

Change description

The **dot1q** keyword was modified to **dot1p**.

Modified feature: Removing the TCP or UDP listening service for a specified VPN instance

Feature change description

From this release, you can remove the TCP or UDP listening service for the specified VPN instance.

Command changes

Modified command: nqa server tcp-connect

Old syntax

undo nqa server tcp-connect *ip-address port-number*

New syntax

undo nqa server tcp-connect *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

The **vpn-instance** keyword was added to the **undo** form of the 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 NQA server listens to the TCP services on the public IP address.

Modified command: nqa server udp-echo

Old syntax

undo nqa server udp-echo *ip-address port-number*

New syntax

undo nqa server udp-echo *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Views

System view

Change description

The **vpn-instance** keyword was added to the **undo** form of the 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 NQA server listens to UDP services on the public IP address.

Modified feature: Configuring the NTP maximum and minimum polling intervals

Feature change description

From this release, the NTP maximum and minimum polling intervals can be configured.

Command changes

Modified command: ntp-service ipv6 unicast-peer

Old syntax

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number*] *

New syntax

ntp-service ipv6 unicast-peer { *peer-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to this command.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

Modified command: ntp-service ipv6 unicast-server

Old syntax

ntp-service ipv6 unicast-server { *server-name* | *ipv6-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number*] *

New syntax

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*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to this command.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

Modified command: ntp-service unicast-peer

Old syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

New syntax

ntp-service unicast-peer { *peer-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*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to this command.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

Modified command: ntp-service unicast-server

Old syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**vpn-instance** *vpn-instance-name*] [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

New syntax

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*] *

Views

System view

Change description

The **maxpoll** *maxpoll-interval* and **minpoll** *minpoll-interval* options were added to this command.

maxpoll *maxpoll-interval*: Specifies the maximum polling interval. The value range for the *maxpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The maximum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *maxpoll-interval* argument is 6 and the default maximum polling interval is 2^6 (64) seconds.

minpoll *minpoll-interval*: Specifies the minimum polling interval. The value range for the *minpoll-interval* argument is 4 to 17, to which base 2 is raised to get the interval in seconds. The minimum polling interval is in the range of 2^4 to 2^{17} (16 to 131072) seconds. The default value for the *minpoll-interval* argument is 6 and the default minimum polling interval is 2^6 (64) seconds.

Modified feature: Configuring an EAA monitor policy interface event

Feature change description

You can configure an EAA monitor policy interface event to monitor an interface list or an interface. Before the modification, only an interface can be monitored.

Command changes

Modified command: event interface

Old syntax

event interface *interface-type interface-number* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

New syntax

event interface *interface-list* **monitor-obj** *monitor-obj* **start-op** *start-op* **start-val** *start-val* **restart-op** *restart-op* **restart-val** *restart-val* [**interval** *interval*]

Views

CLI-defined policy view

Change description

The *interface-type interface-number* argument was changed to *interface-list*.

interface-type interface-number: Specifies an interface by its type and number.

interface-list: Specifies a space-separated list of up to eight interface items. An item specifies an interface or specifies a range of interfaces in the form of *interface-type interface-number* **to** *interface-type interface-number*. The interfaces in an interface range must be the same type. The end interface number must be equal to or greater than the start interface number.

Modified feature: Specifying the DSCP value in log packets sent to the log host

Feature change description

From this release, you can specify the DSCP value in log packets sent to the log host when you configure a log host in the information center.

Command changes

Modified command: info-center loghost

Old syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**facility** *local-number*]

New syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**facility** *local-number*]

Views

System view

Change description

The **dscp** keyword was added.

dscp *dscp-value*: Specifies the DSCP value in log packets sent to the log host. The value range for the *dscp-value* argument is 0 to 63, and the default is 0. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority.

Related documentation

This document introduces software feature changes between HPE 5510HI-CMW710-R3506 and later versions. For information about software feature changes between software versions earlier than HPE 5510HI-CMW710-R3506, see *HPE 5510HI-CMW710-R1311P02 Release Notes (Software Feature Changes)*.