



**Hewlett Packard**  
Enterprise

# HPE 5140EI-CMW710-R6367 Release Notes

The information in this document is subject to change without notice.  
© Copyright 2010, 2024 Hewlett Packard Enterprise Development LP

# Contents

Introduction.....	1
Version information.....	1
Version number.....	1
Version history .....	1
Hardware and software compatibility matrix .....	2
Upgrade restrictions and guidelines.....	3
Hardware feature updates .....	3
5140EI-CMW710-R6367.....	3
5140EI-CMW710-R6363.....	3
5140EI-CMW710-R6351P02 .....	3
5140EI-CMW710-R6351.....	3
5140EI-CMW710-R6343P09 .....	4
5140EI-CMW710-R6343.....	4
5140EI-CMW710-R6337P01 .....	4
5140EI-CMW710-R6330.....	4
5140EI-CMW710-R6327.....	4
5140EI-CMW710-R6325.....	4
Software feature and command updates .....	4
MIB updates .....	4
Operation changes .....	5
Operation changes in R6367 .....	5
Operation changes in R6363 .....	5
Operation changes in R6351P02.....	5
Operation changes in R6351 .....	6
Operation changes in R6343P09.....	6
Operation changes in R6343 .....	6
Operation changes in R6337P01 .....	6
Operation changes in R6330 .....	6
Operation changes in R6327 .....	7
Operation changes in R6325 .....	7
Restrictions and cautions.....	7
Restrictions .....	7
Cautions.....	7

Open problems and workarounds .....	7
List of resolved problems .....	8
Resolved problems in R6367 .....	8
Resolved problems in R6363 .....	8
Resolved problems in R6351P02 .....	10
Resolved problems in R6351 .....	11
Resolved problems in R6343P09 .....	13
Resolved problems in R6343 .....	14
Resolved problems in R6337P01 .....	15
Resolved problems in R6330 .....	17
Resolved problems in R6327 .....	17
Resolved problems in R6325 .....	18
Support and other resources .....	18
Accessing Hewlett Packard Enterprise Support .....	18
Documents .....	19
Related documents .....	19
Documentation feedback .....	19
Appendix A Feature list .....	20
Hardware features .....	20
Software features .....	24
Appendix B Fixed security vulnerabilities .....	27
Fixed security vulnerabilities in R6343 .....	27
Appendix C Upgrading software .....	28
System software file types .....	28
System startup process .....	28
Upgrade methods .....	29
Preparing for the upgrade .....	30
Verifying device status .....	30
Setting up the upgrade environment .....	30
Upgrading from the CLI .....	31
Preparing for the upgrade .....	31
Downloading software images to the master switch .....	32
Upgrading from the Boot menu .....	36
Prerequisites .....	36
Accessing the Boot menu .....	37
Accessing the extended Boot menu .....	38
Upgrading Comware images from the Boot menu .....	39
Upgrading Boot ROM from the Boot menu .....	47

Managing files from the Boot menu .....	54
Handling software upgrade failures.....	57

# List of tables

Table 1 Version history .....	1
Table 2 Hardware and software compatibility matrix .....	2
Table 3 MIB updates .....	4
Table 4 5140EI series hardware features for non-PoE switch models .....	20
Table 5 5140EI series hardware features for non-PoE switch models(2) .....	21
Table 6 5140EI series hardware features for PoE switch models.....	22
Table 7 5140EI series hardware features for PoE switch models(2) .....	23
Table 8 Software features of the 5140EI series .....	24
Table 9 Minimum free storage space requirements.....	36
Table 10 Shortcut keys .....	37
Table 11 Extended Boot ROM menu options.....	38
Table 12 EXTENDED ASSISTANT menu options .....	39
Table 13 TFTP parameter description .....	40
Table 14 FTP parameter description.....	41
Table 15 TFTP parameter description .....	48
Table 16 FTP parameter description.....	49

# Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version HPE 5140EI-CMW710-R6367. 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 5140EI-CMW710-R6367 Release Notes (Software Feature Changes)* and the documents listed in "[Related documents](#)."

## Version information

### Version number

HPE Comware Software, Version 7.1.070, Release 6367

Note: You can see the version number with the command **display version** in any view. Please see **Note ①**.

### 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
5140EI-CMW710-R6367	5140EI-CMW710-R6363	2024-09-12	Release version	Fixed bugs
5140EI-CMW710-R6363	5140EI-CMW710-R6351P02	2024-03-02	Release version	Fixed bugs
5140EI-CMW710-R6351P02	5140EI-CMW710-R6351	2023-10-18	Release version	Fixed bugs
5140EI-CMW710-R6351	5140EI-CMW710-R6343P09	2023-04-01	Release version	Fixed bugs
5140EI-CMW710-R6343P09	5140EI-CMW710-R6343	2022-11-30	Release version	Fixed bugs
5140EI-CMW710-R6343	5140EI-CMW710-R6337P01	2022-06-13	Release version	Fixed bugs
5140EI-CMW710-R6337P01	5140EI-CMW710-R6330	2021-12-09	Release version	Fixed bugs
5140EI-CMW710-R6330	5140EI-CMW710-R6327	2021-05-31	Release version	New feature
5140EI-CMW710-R6327	5140EI-CMW710-R6325	2021-03-01	Release version	Fixed bugs
5140EI-CMW710-R6325	First release	2020-12-25	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	5140EI Series
Hardware platform	HPE 5140 24G 4SFP+ EI Sw JL828A HPE 5140 24G SFP 4SFP+ EI Sw JL826A HPE 5140 48G 4SFP+ EI Sw JL829A HPE 5140 24G PoE+ 4SFP+ EI Sw JL827A HPE 5140 48G PoE+ 4SFP+ EI Sw JL824A HPE 5140 24G PoE+ 2SFP+ 2XGT EI Sw JL823A HPE 5140 48G PoE+ 2SFP+ 2XGT EI Sw JL825A HPE 5140 24G 2SFP+ 2XGT EI Sw R8J41A HPE 5140 8G 2SFP 2GT EI Sw R8J42A
Memory	512M
Flash	256M
Boot ROM version	Version 158 or higher (Note: Use the <b>display version</b> command in any view to view the version information. Please see Note②)
Software images and their MD5 checksums	5140EI-CMW710-R6367.ipe(See the MD5 file)
IMC version	ADNET-FCAPS (E0709) AOM (E0706P01) iMC BIMS 7.3 (E0506H01) iMC EAD7.3 (E0611P10) iMC QoSM 7.3 (E0505P01) iMC EIA 7.3 (E0611P13) iMC PLAT 7.3 (E0705P12) iMC NTA 7.3 (E0707L06) iMC SHM 7.3 (E0707L06)
INode version	iNode PC 7.3 (E0585)
Remarks	N/A

## Display the system software and Boot ROM versions of 5140EI

```
<HPE>display version
```

```
HPE Comware Software, Version 7.1.070, Release 6367 -----Note①
```

```
Copyright (c) 2010-2024 Hewlett Packard Enterprise Development LP
```

```
HPE 5140 24G PoE+ 4SFP+ EI Sw uptime is 0 weeks, 0 days, 0 hours, 2 minutes
```

```
Last reboot reason : Cold reboot
```

```
Boot image: flash:/5140ei-cmw710-boot-r6367.bin
```

```
Boot image version: 7.1.070, Release 6367
Compiled Aug 08 2024 16:00:00
System image: flash:/5140ei-cmw710-system-r6367.bin
System image version: 7.1.070, Release 6367
Compiled Aug 08 2024 16:00:00
```

```
Slot 1:
Uptime is 0 weeks,0 days,0 hours,2 minutes
5140 24G PoE+ 4SFP+ EI Sw with 1 Processor
BOARD TYPE:          5140 24G PoE+ 4SFP+ EI Sw
DRAM:                512M bytes
FLASH:               256M bytes
PCB 1 Version:       VER.A
Bootrom Version:     158          -----Note②
CPLD 1 Version:      001
Release Version:     HPE 5140 24G PoE+ 4SFP+ EI Sw JL827A-6367
Patch Version  :     None
Reboot Cause   :     ColdReboot
[SubSlot 0] 20GE+4COMBO+4SFP Plus
```

## 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

### 5140EI-CMW710-R6367

None.

### 5140EI-CMW710-R6363

None.

### 5140EI-CMW710-R6351P02

None.

### 5140EI-CMW710-R6351

None.



## 5140EI-CMW710-R6343P09

None.

## 5140EI-CMW710-R6343

None.

## 5140EI-CMW710-R6337P01

None.

## 5140EI-CMW710-R6330

Support :

- 5140 24G 2SFP+ 2XGT EI Sw R8J41A
- 5140 8G 2SFP 2GT EI Sw R8J42A

## 5140EI-CMW710-R6327

None.

## 5140EI-CMW710-R6325

First release.

# Software feature and command updates

For more information about the software feature and command update history, see *HPE 5140\_EI-CMW710-R6367 Release Notes (Software Feature Changes)*.

## MIB updates

Table 3 MIB updates

Item	MIB file	Module	Description
<b>5140EI-CMW710-R6367</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6363</b>			
New	None	None	None
Modified	None	None	None

Item	MIB file	Module	Description
<b>5140EI-CMW710-R6351P02</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6351</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6343P09</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6343</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6337P01</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6330</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6327</b>			
New	None	None	None
Modified	None	None	None
<b>5140EI-CMW710-R6325</b>			
New	First release	First release	First release
Modified	First release	First release	First release

## Operation changes

### Operation changes in R6367

None.

### Operation changes in R6363

support ipv6 ready.

### Operation changes in R6351P02

None.

## Operation changes in R6351

Changed the length of the attribute name string carried in a RADIUS packet from 64 characters to 253 characters.

## Operation changes in R6343P09

None.

## Operation changes in R6343

**The number of available ACL resources was increased from 512 to 768.**

**Change for the ipv6 verify source ip-address mac-address command.**

- Before modification: The device will generate **four** permit ACL rules and **one** deny ACL rule for each interface on which the **ipv6 verify source ip-address mac-address** command is executed. The total number of used resources is the number of interfaces multiplied by (4+1).
- After modification: The device will generate **four** permit ACL rules for all configured interfaces globally and generate one deny ACL rule for each interface. The total number of used resources is the number of interfaces multiplied by 1 plus 4.

**Change for the igmp-snooping source-deny command.**

- Before modification: The device will generate **one** permit ACL rule and **one** deny ACL rule for each interface on which the **igmp-snooping source-deny** command is executed. The total number of used resources is the number of interfaces multiplied by (1+1).
- After modification: The device will generate **one** permit ACL rule for all configured interfaces globally and generate one deny ACL rule for each interface. The total number of used resources is the number of interfaces multiplied by 1 plus 1.

**Change for the mld-snooping source-deny command.**

- Before modification: The device will generate **three** permit ACL rules and **one** deny ACL rule for each interface on which the **mld-snooping source-deny** command is executed. The total number of used resources is the number of interfaces multiplied by (3+1).
- After modification: The device will generate **three** permit ACL rules for all configured interfaces globally and generate one deny ACL rule for each interface. The total number of used resources is the number of interfaces multiplied by 1 plus 3.

## Operation changes in R6337P01

None.

## Operation changes in R6330

**On an IRF fabric that has multiple IRF physical links, the packet loss duration has decreased after you shut down and then bring up one IRF physical interface.**

- Before modification: The packet loss duration is longer than 2000 milliseconds.
- After modification: The packet loss duration is in the range of 200 to 500 milliseconds.

# Operation changes in R6327

None.

# Operation changes in R6325

First release.

## Restrictions and cautions

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.

When you use this version of software, make sure you fully understand the restrictions and cautions described in this section.

## Restrictions

Release 6367 must use BootROM 158 or a later version.

If data packets are assigned to queue 7 and the scheduling algorithm is SP, all packets sent from the CPU are affected.

To avoid false alarms, make sure the statistics collection and comparison interval for CRC error packets configured in the **ifmonitor crc-error** command is greater than 15 seconds.

Not Support SmartMC.

## Cautions

None.

## Open problems and workarounds

### 202409061705

- Symptom: On the Web interface, the month and the dropdown icon overlap.
- Condition: This symptom occurs when you set the time on the Web interface.
- Workaround: None.

### 202408141649

- Symptom: The value ranges for the secure MAC aging timer are different on the Web interface and at the CLI.
- Condition: This symptom occurs if you set the secure MAC aging timer in seconds at the CLI.
- Workaround: Set the secure MAC aging timer in minutes at the CLI.

# List of resolved problems

## Resolved problems in R6367

### 202408151048

- Symptom: No MAC address entry is added and no trap about deleting a node is reported when a MAC address moves.
- Condition: This symptom occurs if a MAC address moves from the first port to the second port.

### 202407160651

- Symptom: After the startup, a user cannot log in with the password, but can log in with an empty password and is required to change the password.
- Condition: This symptom might occur if the device finishes the version upgrade, saves the configuration again, and restarts after the password control feature is enabled. The restart recovers the configuration through the configuration file by deleting the .mdb file or a version update. In addition, the lauthd process restarts, or the device restarts after the save operation.

### 202407090199

- Symptom: The poe max-power command cannot be configured after the device power cycles.
- Condition: This symptom might occur if the device power cycles.

### 202403180789

- Symptom: PTP time synchronization fails if VLANs are inconsistent between the master and member clocks.
- Condition: This symptom might occur if VLANs are inconsistent between the master and member clocks in PTP.

### 202408120285

- Symptom: The ifmonitor command fails to be configured on a multi-rate interface.
- Condition: This symptom might occur if you configure the ifmonitor command on a multi-rate interface.

### 202404110742

- Symptom: The device might report MIB node information about power supply failure if SNMP is enabled on the device.
- Condition: This symptom might occur if SNMP is enabled on the device.

## Resolved problems in R6363

### 202307030467

- Symptom: The VLAN deployed by iMC fails to be configured.
- Condition: This symptom occurs if a VLAN with member ports already exists on the device and then the VLAN is deployed from iMC.

### 202312041375

- Symptom: The firmware is lost after the device is power cycled.
- Condition: This symptom occurs if the device is power cycled.

**202311240127**

- Symptom: Temperature alarms are mistakenly reported.
- Condition: None.

**202311240114**

- Symptom: PTP packets cannot be transparently transmitted.
- Condition: None.

**202311101350**

- Symptom: The management port flaps.
- Condition: This symptom occurs if the management port runs for a long time.

**202311240102**

- Symptom: The subordinate device on an IRF fabric does not generate an alarm for the hh3cStackPortLinkStatusChange node when the master device is powered off.
- Condition: This symptom occurs when the master device is powered off.

**202307211617**

- Symptom: Failed to enable the HTTPS service by using the ip https enable command.
- Condition: This symptom occurs when the device has configured with the restful http enable or restful https enable command.

**202309071883**

- Symptom: When you conduct cable detection on certain Ethernet ports of the device, it prompts that this feature is not supported.
- Condition: This symptom might occur if you use the virtual-cable-test command to conduct cable detection on Ethernet ports.

**202309071086**

- Symptom: The device restarts unexpectedly.
- Condition: This symptom might occur if the peer port continues to emit and extinguish light after the local fiber port is shut down.

**202308161212**

- Symptom: The port\_block ACL is not deleted, and ARP packets cannot be forwarded.
- Condition: This symptom occurs if multiple Layer 2 protocols set an interface to the blocked state at the same time and then recover the interface to the forwarding state.

**202307110941**

- Symptom: If you apply MQC with remark local-precedence behavior to multiple ports (on different forwarding chips) on a dual-chip device, undoing MQC on one port also invalidates the MQC applied to ports on the other chip.
- Condition: This symptom might occur after you perform the following:
  - Apply MQC with remark local-precedence behavior to multiple ports (on different forwarding chips) on a dual-chip device.
  - Undo MQC on one port.

**202308220092**

- Symptom: 100-Mbps transceiver modules cannot come up.
- Condition: This symptom occurs if a 1000-Mbps transceiver module is installed in a fiber port on the front panel.

#### **202307140367**

- Symptom: The display rules for IPv6 addresses are inconsistent. Some IPv6 addresses support abbreviation, while others don't.
- Condition: This symptom occurs if the device is configured with IPv6 addresses.

#### **202307051264**

- Symptom: The device does not display logs for adding MAC address entries and displays logs only for deleting MAC address entries.
- Condition: This symptom occurs if you configure port security settings on a port and connect the port to the peer end.

#### **202306160696**

- Symptom: The display qos-acl resource command shows that some ACL resources are not released after the many-to-one VLAN mapping configuration is deleted or the interface is shut down.
- Condition: This symptom occurs if the following operations are performed:
  - Configure many-to-one VLAN mapping on an interface.
  - After traffic with the original VLAN tag is present on the interface for a period of time, delete the many-to-one VLAN mapping configuration or shut down the interface.

#### **202306071059**

- Symptom: The configuration cannot be saved when factory defaults are restored.
- Condition: This symptom occurs when you restore factory defaults.

#### **202305112068**

- Symptom: When you execute the display mac-address command to display MAC address entries, the Aging field for a MAC address entry that can age out displays N instead of Y.
- Condition: This symptom occurs if the user of the MAC address in the entry comes online through MAC authentication.

#### **202303030834**

- Symptom: You cannot log in to the device after command accounting is configured.
- Condition: This symptom occurs if the remote server for command accounting is unavailable.

#### **202303060450**

- Symptom: After the device obtains an IPv6 address through DHCP, no default route is generated.
- Condition: This symptom might occur if the device obtains an IPv6 address through DHCP.

#### **202303280516**

- Symptom: When the RADIUS authentication server for 802.1X authentication is unreachable, users cannot bypass authentication through the none authentication method.
- Condition: This symptom occurs if the RADIUS authentication server is unreachable and the none authentication method is used.

## **Resolved problems in R6351P02**

None.

# Resolved problems in R6351

## 202303162097

- Symptom: The IRF fabric reboots because the memory is exhausted.
- Condition: This symptom occurs if a master/subordinate switchover is performed or a DHCP client requests multiple addresses from the IRF fabric acting as a DHCP relay.

## 202303151120

- Symptom: The DHCP process exits unexpectedly and then recovers after DHCP relay entries are aged out.
- Condition: This symptom occurs if the following conditions exist:
  - The switch acts as a DHCP relay.
  - A DHCP client obtains two IP addresses on an interface and then obtained one of the two addresses on another interface.
  - The DHCP relay entries are aged out.

## 202303130217

- Symptom: The switch reboots when LAGG/LoadSharing information is obtained through NETCONF.
- Condition: This symptom occurs when LAGG/LoadSharing information is obtained through NETCONF.

## 202303010469

- Symptom: Failed to log in to the switch through HTTP or HTTPS.
- Condition: This symptom occurs if the RADIUS server issues the Login-Service attribute to the switch during RADIUS authentication.

## 202302280994

- Symptom: The switch reboots when the **display diagnostic-information** command is executed.
- Condition: This symptom occurs when the **display diagnostic-information** command is executed.

## 202302270992

- Symptom: An IRF fabric cannot be formed.
- Condition: This symptom occurs if you use 10-GE copper ports as IRF ports and set the IRF link down report delay to 0.

## 202302140409

- Symptom: When you use SNMP to read the value of the hh3cEntityExtErrorStatus MIB object, the status of the fixed power supply is not returned.
- Condition: This symptom occurs if you use SNMP to read the value of the hh3cEntityExtErrorStatus MIB object.

## 202302141134

- Symptom: A memory alarm is generated.
- Condition: This symptom occurs if you execute the **vcf-fabric topology enable** command and an interface goes down and comes up frequently.



## 202302151892

- Symptom: The **display power** and **display device manuinfo** commands cannot display the corresponding output. The **reboot** command is stuck at **Now rebooting, please wait**.
- Condition: This symptom occurs when you execute the **display power**, **display device manuinfo**, or **reboot** command.

## 202212070008

- Symptom: After a device reboots, it does not have IPv6 connectivity.
- Condition: This symptom might occur when the following conditions exist:
  - The device receives a large number of IPv6 packets from unknown addresses after reboot.
  - The device protects its CPUs against packet attacks by default.

## 202212070538

- Symptom: The system printed the log message of deleting MAC address 0000-0000-0000.
- Condition: This symptom occurs if the following conditions exist on an IRF fabric:
  - Port 0 exists on the device.
  - When a port is configured with port security and learns MAC addresses, the port flaps or receives TC packets.

## 202211141586

- Symptom: The offline detection or ARP detection function for 802.1X users is abnormal, and users cannot age out to go offline.
- Condition: This symptom occurs if the authorization VLAN is modified on the authentication server after 802.1X users successfully come online.

## 202210280272

- Symptom: The device memory leaks.
- Condition: This symptom occurs if the NETCONF controller frequently subscribes to events and cancels event subscriptions for the device.

## 202210141030

- Symptom: The device cannot process new NETCONF requests.
- Condition: This symptom occurs if an event subscription cancellation request is sent to the device when the subscribed NETCONF events are being reported.

## 202210120883

- Symptom: The NTP packets are sent to the CPU for processing. As a result, NTP packets cannot be forwarded normally, and NTP cannot synchronize the time.
- Condition: This symptom occurs if the device acts as a gateway to forward NTP packets through a Layer 3 interface.

## 202209220968

- Symptom: When an endpoint receives an IP address allocated by the DHCP server, the device initiates gratuitous ARP packets within the network for IP address conflict detection. No replies are received from the network, which means that no address conflict exists. However, the endpoint replies to the DHCP server with a DHCP-DECLINE packet to apply for an IP address again. As a result, the endpoint repeatedly obtains an IP address.
- Condition: This symptom occurs if the **arp suppression** or **arp snooping** command is executed on the device.

#### 202208130589

- Symptom: Executing the reset kernel deadlock, reset kernel exception, reset kernel reboot, or reset kernel starvation command cannot clear the corresponding information.
- Condition: This symptom occurs when you execute the reset kernel deadlock, reset kernel exception, reset kernel reboot, or reset kernel starvation command.

#### 202208050249

- Symptom: The device cannot learn routing entries.
- Condition: This symptom occurs if a QoS policy containing a large number of class-based accounting actions is applied.

#### 202207010954

- Symptom: The configured remote ID of Option 82 is not displayed in the **display dhcp relay information** command output.
- Condition: This symptom occurs if you configure the padding format is hex and the remote ID starts with 0.

#### 202206201644

- Symptom: The switch fails to forward IPv6 ICMP packets at Layer 2.
- Condition: This symptom occurs if the source IPv6 address of the packet contains abc0, for example, 2001:250:100d:abcd::abcd.

## Resolved problems in R6343P09

#### 202206140089

- Symptom: On an IRF fabric, the MAC address of a packet forwarded across member devices cannot be learned.
- Condition: This symptom occurs if the logical interface number of the service port is the same as that of the IRF port.

#### 202208230885

- Symptom: Port 80 and port 443 are not deleted after the HTTP service and HTTPS service are disabled.
- Condition: This symptom occurs after the HTTP service and HTTPS service are disabled.

#### 202208040367

- Symptom: The power LED is solid yellow, and the power supply status is Fault in the display power command output.
- Condition: This symptom occurs if a Great Wall 150-W power supply is used on the device.

#### 202206210164

- Symptom: Intrusion protection is not triggered when an interface receives packets from a learned MAC address.
- Condition: This symptom occurs if the following operations have been performed:
  - a. Enable port security.
  - b. On each of two interfaces, set the maximum number of secure MAC addresses allowed to 1.
  - c. Send packets from the learned MAC address to one of the two interfaces.

# Resolved problems in R6343

## 202204210856

- Symptom: The fiber port of the combo port is up.
- Condition: This symptom occurs when the copper port of the fiber converter connected to the device is down.

## 202205090269

- Symptom: The switch fails to supply power to some nonstandard PDs (such as Cisco 7940G IP phone) through PoE.
- Condition: This symptom might occur after PoE and nonstandard PD detection are enabled on the switch.

## 202205050956

- Symptom: In the output from the **display irf link** command, the IRF physical interface on a standby MPU is displayed as down even if the interface is up.
- Condition: This symptom might occur if the IRF port on the standby MPU flaps constantly.

## 202204130283

- Symptom: When the display mac-address command is executed to view the MAC address table, the latest entries are not displayed. The MAC address learning limit configuration cannot be deleted. After an interface goes down, it is still displayed as up.
- Condition: This symptom occurs if the MAC address learning limit is set to 1 on an interface, and a MAC address moves to the interface.

## 202204080241

- Symptom: Failed to obtain the SN of a transceiver module.
- Condition: This symptom occurs if you obtain the MIB information of a transceiver module through SNMP.

## 202203300985

- Symptom: The subordinate IRF member device might fail to start normally.
- Condition: This symptom might occur if a master/subordinate switchover is performed on an IRF fabric with a large amount of configuration.

## 202203170120

- Symptom: The CPU usage of the device is high.
- Condition: This symptom occurs if a transceiver module is repeatedly shut down and brought up.

## 202201140229

- Symptom: The PoE interface that supplies power is not the one configured.
- Condition: This symptom occurs if the following conditions exist:
  - The PoE daughter card used on the device is LSPPSE48A, LSPPSE24A, LSPPSE16A, or LSPPSE8A. To view the PoE daughter card model, execute the **display poe pse** command. The value of the **PSE Model** field in the command output is the PoE daughter card model.
  - The **poe enable** command has been executed.

## 202202231179

- Symptom: Only SNMPv3 takes effect on the device after SNMPv1, SNMPv2c, and SNMPv3 are all configured.

- Condition: This symptom occurs if the following conditions exist:
  - The device starts up with the factory defaults.
  - Use the **snmp-agent sys-info version all** command to specify SNMPv1, SNMPv2c, and SNMPv3 for the device.

#### 202203010889

- Symptom: Slow to obtain information from the **IldpV2RemSysName** MIB object.
- Condition: This symptom occurs if you request the value of the **IldpV2RemSysName** MIB object remotely.

#### 202201250424

- Symptom: Unknown packets cannot be flooded to router ports, and multicast forwarding is abnormal.
- Condition: This symptom occurs if you use the **igmp-snooping drop-unknown** command to enable dropping unknown multicast data packets and disable IGMP snooping for a VLAN on the Layer 2 device of the multicast source.

#### 202201040567

- Symptom: The flow control function cannot work when the device is connected to a PC.
- Condition: This symptom occurs when the device is connected to a PC.

#### 202103250327

- Symptom: When the device is running, the network management interface might go down and cannot be recovered.
- Condition: This symptom occurs if the network management interface repeatedly sends and receives packets.

#### 202112230657

- Symptom: The CPU usage is always high. The **display mac-address** command cannot display information normally.
- Condition: This symptom occurs if MAC address entries are frequently added and deleted.

## Resolved problems in R6337P01

#### 202111150249

- Symptom: The device has a deadlock reboot.
- Condition: This symptom occurs if you execute **shutdown** and **undo shutdown** commands repeatedly on the peer ports, causing flapping of the local ports.

#### 202111050868

- Symptom: The CPU usage of the device reaches 75%.
- Condition: This symptom occurs if you enable accounting for charging, execute the **repeat** command, and then restart the UCM process on the device.

#### 202109241082

- Symptom: After the device's system time is synchronized, an SSH user fails to log in to the device and gets a prompt of "Failed to login because the idle timer expired."
- Condition: This symptom occurs when the following conditions are met:
  - The password control feature is enabled.
  - The maximum account idle time is not 0 (set by the **password-control login idle-time** command).

- The system time is too early and the SSH user has logged in to the device before.
- The system time is changed to the current time.

#### **202110090340**

- Symptom: The device reboots unexpectedly.
- Condition: This symptom occurs if the mac-vlan enable command is executed to enable the MAC-based VLAN feature on a port and then the mac-vlan trigger enable command is executed to enable dynamic MAC-based VLAN assignment on the port.

#### **202110090688**

- Symptom: Failed to ping a PC from an interface after the network cable is removed from and then re-inserted into the interface.
- Condition: This symptom occurs if port security has been configured on the interface.

#### **202107050836**

- Symptom: The device CPU usage is high.
- Condition: This symptom occurs if an SNMP request for transceiver module information fails.

#### **202109011682**

- Symptom: Packets are lost when they are forwarded through PBR.
- Condition: This symptom occurs when you specify both the input and output interfaces in the PBR policy on chip 1 of the device configured with two switching chips.

#### **202107211516**

- Symptom: The Circuit ID field in the display dhcp snooping information command output is empty.
- Condition: This symptom occurs if you configure the padding mode for the Circuit ID sub-option of Option 82 as normal-extended.

#### **202106250033**

- Symptom: MAC addresses are not aged out based on the aging time configured in port security.
- Condition: This symptom occurs if the following conditions exist:
  - Port security is enabled globally.
  - Users come online on one port and then move to another port.

#### **202107290628**

- Symptom: sFlow cannot collect interface counter information in time, and the collected traffic rate for fixed-rate traffic is not fixed.
- Condition: This symptom occurs if you enable sFlow on an interface and use an sFlow collector to analyze collected packets.

#### **202104210763**

- Symptom: When the DHCP server cannot find an assignable IP address in the primary network segment, the DHCP client cannot obtain an IP address from the secondary network segments.
- Condition: This symptom occurs when the following conditions exist:
  - The DHCP server is configured with an IP address pool that has a primary network segment and secondary network segments.
  - The DHCP client requests an IP address when the DHCP server has no assignable IP address in the primary network segment.

#### **202105310255**

- Symptom: The NMS failed to deploy VLAN configuration to a device.

- Condition: This symptom occurs if the VLAN configuration to be deployed by the NMS is the same as that on the device.

#### **202104200312**

- Symptom: A MAC authentication user might fail to come online.
- Condition: This symptom occurs if the following conditions exist:
  - Both 802.1X authentication and MAC authentication are enabled on an interface.
  - The 802.1X guest VLAN is configured on the interface.
  - After a MAC authentication successfully comes online, the user repeatedly goes offline and comes online.

## **Resolved problems in R6330**

#### **202104131824**

- Symptom: On an IRF system, after the MAC address entry for a voice VLAN ages out on the subordinate member device, the downlink traffic will be broadcast on the subordinate member device.
- Condition: This symptom occurs if the traffic matching the MAC address entry for the voice VLAN is initiated on the master member device and the MAC address entry age out because no traffic matches the MAC address entry within one aging period on the subordinate member device.

#### **202104190149**

- Symptom: The traffic reported by sFlow is different from the actual traffic on a port.
- Condition: This symptom occurs if sFlow sampling is enabled on the device.

#### **202105280911**

- Symptom: On a device with two chips, sFlow cannot sample traffic on ports of chip 1.
- Condition: This symptom occurs if you first configure sFlow sampling for traffic on ports of chip 0 and then for traffic on ports of chip 1 on a device with two chips.

#### **202101181488**

- Symptom: Forwarding error exists for packets with a destination MAC address that hits a multiport unicast MAC address entry on an IRF fabric.
- Condition: This symptom occurs if the following conditions exist:
  - The packets are received on a subordinate device in the IRF fabric.
  - The multiport unicast MAC address entry that the packets hit is synchronized from the master device to the subordinate device.

#### **202101181303**

- Symptom: On the device configured with an isolation group and ARP snooping, a port in the isolation group forwards an ARP packet received from another port in the isolation group.
- Condition: This symptom occurs if the device receives an ARP packet on a port in the isolation group.

## **Resolved problems in R6327**

#### **202101151443**

- Symptom: Logging is enabled for portal user logins and logouts on the device. When the device is accessed from IMC, the IMC system log page fails to load.

- Condition: This symptom might occur if the following conditions exist:
  - Logging is enabled for portal user logins and logouts on the device.
  - Transparent MAC authentication is enabled on IMC, or the iNode client is enabled to upload the client version number.

#### 202101130494

- Symptom: The display mac-address command displays duplicate MAC address entries for a MAC address.
- Condition: This symptom might occur if the following operations are performed:
  - a. Configure a multiport MAC address entry to overwrite a dynamic MAC address entry.
  - b. Execute the **undo mac-address** command to delete the multiport MAC address entry.
  - c. Wait for the device to learn the MAC address dynamically.

#### 202101080488

- Symptom: If IPSG is enabled on a VLAN interface, the IPv4SG bindings fail to be issued.
- Condition: This symptom occurs if IPSG is enabled on a VLAN interface.

#### 202012241455

- Symptom: A marking-type QoS policy applied globally does not take effect after its traffic behaviors are modified.
- Condition: This symptom occurs if a marking-type QoS policy is applied globally and then its traffic behaviors are modified.

## Resolved problems in R6325

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](http://www.hpe.com/assistance)
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:  
[www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)

Information to collect:

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

# Documents

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

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

## Related documents

The following documents provide related information:

- HPE FlexNetwork 5140 EI Switch Series Configuration Guides-R63xx
- HPE FlexNetwork 5140 EI Switch Series Command References-R63xx
- HPE FlexNetwork 5140 EI Switch Series Installation Guide

## 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](mailto:docsfeedback@hpe.com)). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.



# Appendix A Feature list

## Hardware features

**Table 4 5140EI series hardware features for non-PoE switch models**

Item	5140 24G 4SFP+ EI Sw	5140 48G 4SFP+ EI Sw	5140 24G SFP 4SFP+ EI Sw
Dimensions (H x W x D)	43.6 x 440 x 160 mm (1.72 x 17.32 x 6.30 in)	43.6 x 440 x 230 mm (1.72 x 17.32 x 9.06 in)	43.6 x 440 x 360 mm (1.72 x 17.32 x 14.17 in)
Weight	≤ 2.5 kg (5.51 lb)	≤ 3.5 kg (7.72 lb)	≤ 6.5 kg (14.33 lb)
Console port	1 x serial console port 1 x micro USB console port  When both ports are connected, only the micro USB console port is available.	1 x serial console port 1 x micro USB console port  When both ports are connected, only the micro USB console port is available.	1 x serial console port 1 x micro USB console port  When both ports are connected, only the micro USB console port is available.
10/100/1000B ASE-T autosensing Ethernet port	24	48	8 (Each and its corresponding SFP port form a combo interface.)
SFP port	N/A	N/A	24 (The rightmost eight SFP ports form a combo interface with their corresponding 10/100/1000BASE-T autosensing Ethernet ports, respectively.)
SFP+ port	4	4	4
Power module slot	N/A	N/A	2, at the rear panel
Input voltage	<ul style="list-style-type: none"> <li>Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz</li> <li>Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz</li> </ul>		<p>PSR75-12A:</p> <ul style="list-style-type: none"> <li>Rated voltage: <ul style="list-style-type: none"> <li>100 VAC to 240 VAC @ 50 or 60 Hz</li> <li>240 VDC</li> </ul> </li> <li>Max voltage: <ul style="list-style-type: none"> <li>90 VAC to 290 VAC @ 47 to 63 Hz</li> <li>180 to 320 VDC</li> </ul> </li> </ul> <p>PSR150-A1:</p> <ul style="list-style-type: none"> <li>Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz</li> <li>Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz</li> </ul> <p>PSR150-D1:</p> <ul style="list-style-type: none"> <li>Rated voltage: -48 VDC to -60 VDC</li> <li>Max voltage: -36 VDC to -72 VDC</li> </ul> <p>DC power source for the</p>

			PSR150-D1 power module: -48 VDC power source in the equipment room or an RPS (H3C RPS800-A or RPS1600-A)
Minimum power consumption	10 W	19 W	1 × PSR75-12A: 15 W 2 × PSR75-12A: 17 W 1 × PSR150-A1: 18 W 1 × PSR150-D1: 18 W 2 × PSR150-A1: 23 W 2 × PSR150-D1: 22 W
Maximum power consumption	24 W	44 W	1 × PSR75-12A: 45 W 2 × PSR75-12A: 48 W 1 × PSR150-A1: 48 W 1 × PSR150-D1: 51 W 2 × PSR150-A1: 55 W 2 × PSR150-D1: 57 W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943		
Melting current of power module fuse	2 A/250 V	3.15 A/250 V	PSR75-12A: 3.15 A/250 V PSR150-A1: 6.3 A/250 V PSR150-D1: 8 A/250 V
Cooling system	Using fixed fan trays to draw ambient air in from the left side, right side, and port side of the chassis and exhaust heated air out from the power module side	Using fixed fan trays to draw ambient air in from the left side and exhaust heated air out from the right side and power module side	Using fixed fan trays to draw ambient air in from the left side and port side and exhaust heated air from the right side
Operating temperature	-5° C ~ 45° C (23°F to 113°F)		
Operating humidity	5% to 95%, noncondensing		
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943		

**Table 5 5140EI series hardware features for non-PoE switch models(2)**

Item	5140 24G 2SFP+ 2XGT EI Sw	5140 8G 2SFP 2GT EI Sw
Dimensions (H × W × D)	43.6 × 440 × 160 mm (1.72 × 17.32 × 6.30 in)	43.6 × 266 × 161 mm (1.72 × 10.47 × 6.34 in)
Weight	≤ 2.5 kg (5.51 lb)	≤ 1.5 kg (3.31 lb)
Console port	1 × serial console port	
10/100/1000B ASE-T autosensing Ethernet port	24	10 (The rightmost two form a combo interface with their corresponding SFP ports, respectively.)
1/10GBase-T autosensing Ethernet port	2	N/A

SFP port	N/A	4 (The leftmost two form a combo interface with their corresponding 10/100/1000BASE-T autosensing Ethernet ports, respectively.)
SFP+ port	2	N/A
Input voltage	Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz	
Minimum power consumption	14W	8 W
Maximum power consumption	36W	15 W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	
Melting current of power module fuse	2 A/250 V	
Cooling system	Using fixed fan trays to draw ambient air in from the left side and exhaust heated air from the right side	Natural cooling without fan trays
Operating temperature	-5°C ~ 45°C (23°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	

**Table 6 5140EI series hardware features for PoE switch models**

Item	5140 48G PoE+ 4SFP+ EI Sw	5140 24G PoE+ 4SFP+ EI Sw
Dimensions (H × W × D)	43.6 × 440 × 400 mm (1.72 × 17.32 × 15.75 in)	43.6 × 440 × 260 mm (1.72 × 17.32 × 10.24 in)
Weight	≤ 6 kg (13.23 lb)	≤ 4.5 kg (9.92 lb)
Console port	<ul style="list-style-type: none"> <li>1 × serial console port</li> <li>1 × micro USB console port</li> <li>When both ports are connected, only the micro USB console port is available.</li> </ul>	
10/100/1000BASE-T autosensing Ethernet port	48	24 (The four highest-numbered 10/100/1000BASE-T autosensing Ethernet ports form combo interfaces with their corresponding SFP ports, respectively.)
SFP port	N/A	4 (Each and its corresponding 10/100/1000BASE-T autosensing Ethernet port form a combo interface.)
SFP+ port	4	
Input voltage	AC power source: <ul style="list-style-type: none"> <li>Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz</li> <li>Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz</li> </ul>	

	DC power source: H3C RPS1600-A <ul style="list-style-type: none"> <li>Rated voltage: -54 VDC to -57 VDC</li> <li>Max voltage:               <ul style="list-style-type: none"> <li>Single DC input: -44 VDC to -60 VDC</li> <li>AC and DC inputs: -54 VDC to -57 VDC</li> </ul> </li> </ul>	
Maximum PoE power per port	30 W	
Total PoE power	AC: 370 W DC: 740 W	
Minimum power consumption	AC: 37 W DC: 29 W	AC: 24 W DC: 17 W
Maximum power consumption (including PoE power consumption)	AC: 478 W DC: 825 W	AC: 451 W DC: 793 W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	
Melting current of power module fuse	15 A/250 V	
Cooling system	Using fixed fan trays to draw ambient air in from the left side and exhaust heated air from the right side	Using fixed fan trays to draw ambient air in from the left side and port side and exhaust heated air from the right side
Operating temperature	-5° C~45° C (23°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	

**Table 7 5140EI series hardware features for PoE switch models(2)**

Item	5140 24G PoE+ 2SFP+ 2XGT EI Sw	5140 48G PoE+ 2SFP+ 2XGT EI Sw
Dimensions (H x W x D)	43.6 x 440 x 320 mm (1.72 x 17.32 x 12.60 in)	43.6 x 440 x 320 mm (1.72 x 17.32 x 12.60 in)
Weight	≤4.5kg (9.92 lb)	≤4.5 kg (9.92 lb)
Console port	<ul style="list-style-type: none"> <li>1 x serial console port</li> </ul>	
10/100/1000BA SE-T autosensing Ethernet port	24	48
1/10GBase-T autosensing Ethernet port	2	2
SFP+ port	2	2
Input voltage	<ul style="list-style-type: none"> <li>Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz</li> <li>Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz</li> </ul>	

Maximum PoE power per port	30 W	
Total PoE power	370W	
Minimum power consumption	20W	32W
Maximum power consumption (including PoE power consumption)	450W	470W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	
Melting current of power module fuse	2 A/250 V	2 A/250 V
Cooling system	Using fixed fan trays to draw ambient air in from the left side and exhaust heated air from the right side	
Operating temperature	-5° C~45° C (23°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	

## Software features

**Table 8 Software features of the 5140EI series**

Feature	5140EI series switch
IRF	<ul style="list-style-type: none"> <li>• Ring topology</li> <li>• Daisy chain topology</li> <li>• LACP MAD</li> <li>• ARP MAD</li> </ul>
Link aggregation	<ul style="list-style-type: none"> <li>• Aggregation of 1-GE ports</li> <li>• Aggregation of 10-GE ports</li> <li>• Static link aggregation</li> <li>• Dynamic link aggregation</li> <li>• Inter-device aggregation</li> <li>• A maximum of 14 aggregation groups on a device</li> <li>• A maximum of 124 inter-device aggregation groups</li> <li>• A maximum of 8 ports for each aggregation group</li> </ul>
Flow control	<ul style="list-style-type: none"> <li>• IEEE 802.3x flow control</li> </ul>
Jumbo Frame	<ul style="list-style-type: none"> <li>• Supports maximum frame size of 10000</li> </ul>
MAC address table	<ul style="list-style-type: none"> <li>• 16K MAC addresses</li> <li>• 1K static MAC addresses</li> <li>• Blackhole MAC addresses</li> <li>• MAC address learning limit on a port</li> </ul>

VLAN	<ul style="list-style-type: none"> <li>• Port-based VLANs (4094 VLANs)</li> <li>• QinQ</li> <li>• VLAN mapping</li> </ul>
ARP	<ul style="list-style-type: none"> <li>• 1K entries</li> <li>• 512 static entries</li> <li>• Gratuitous ARP</li> <li>• ARP black hole</li> <li>• ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings)</li> <li>• ARP source suppression</li> </ul>
ND	<ul style="list-style-type: none"> <li>• 240 entries</li> <li>• 128 static entries</li> </ul>
VLAN virtual interface	<ul style="list-style-type: none"> <li>• 32</li> </ul>
DHCP	<ul style="list-style-type: none"> <li>• DHCP client</li> <li>• DHCP snooping</li> <li>• DHCP relay</li> <li>• DHCP server</li> <li>• DHCPv6 Server</li> <li>• DHCPv6 relay</li> <li>• DHCPv6 snooping</li> </ul>
UDP Helper	<ul style="list-style-type: none"> <li>• UDP Helper</li> </ul>
DNS	<ul style="list-style-type: none"> <li>• Static DNS</li> <li>• Dynamic DNS</li> <li>• IPv4 and IPv6 DNS</li> </ul>
unicast route	<ul style="list-style-type: none"> <li>• IPv4 and IPv6 static routes</li> <li>• RIP/RIPng</li> <li>• OSPF/OSPFv3</li> <li>• Routing policies</li> <li>• Policy-based routing</li> <li>• IPv6 policy-based routing</li> </ul>
Multicast	<ul style="list-style-type: none"> <li>• IGMP snooping</li> <li>• PIM Snooping</li> <li>• MLD snooping</li> <li>• IPv4 and IPv6 multicast VLAN</li> <li>• IPv6 PIM Snooping</li> </ul>
Broadcast/multicast/unicast storm control	<ul style="list-style-type: none"> <li>• Storm control based on port rate percentage</li> <li>• PPS-based storm control</li> <li>• Bps-based storm control</li> </ul>
MSTP	<ul style="list-style-type: none"> <li>• STP/RSTP/MSTP protocol</li> <li>• STP Root Guard</li> <li>• BPDU Guard</li> <li>• 128 PVST instances</li> </ul>
QoS/ACL	<ul style="list-style-type: none"> <li>• Remarking of 802.1p and DSCP priorities</li> <li>• Packet filtering at L2 (Layer 2) through L4 (Layer 4)</li> <li>• Eight output queues for each port</li> <li>• SP/WRR/SP+WRR queue scheduling algorithms</li> <li>• Port-based rate limiting</li> <li>• Flow-based redirection</li> <li>• Time range</li> </ul>

Mirroring	<ul style="list-style-type: none"> <li>• Stream mirroring</li> <li>• Port mirroring</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Hierarchical management and password protection of users</li> <li>• AAA authentication</li> <li>• RADIUS authentication</li> <li>• HWTACACS</li> <li>• LDAP</li> <li>• SSH 2.0</li> <li>• Port isolation</li> <li>• 802.1X</li> <li>• Portal</li> <li>• Port security</li> <li>• MAC-address-based authentication</li> <li>• IP Source Guard</li> <li>• HTTPS</li> <li>• PKI</li> <li>• IPsec</li> <li>• EAD</li> <li>• Public key management</li> </ul>
802.1X	<ul style="list-style-type: none"> <li>• Up to 2K users</li> <li>• Port-based and MAC address-based authentication</li> <li>• Trunk port authentication</li> <li>• Dynamic 802.1X-based QoS/ACL/VLAN assignment</li> </ul>
Loading and upgrading	<ul style="list-style-type: none"> <li>• Loading and upgrading through XModem protocol</li> <li>• Loading and upgrading through FTP</li> <li>• Loading and upgrading through the trivial file transfer protocol (TFTP)</li> </ul>
Management	<ul style="list-style-type: none"> <li>• Configuration at the command line interface</li> <li>• Remote configuration through Telnet</li> <li>• Configuration through Console port</li> <li>• Simple network management protocol (SNMP)</li> <li>• Remote Monitoring(RMON)</li> <li>• IMC NMS</li> <li>• System log</li> <li>• Hierarchical alarms</li> <li>• NTP</li> <li>• Power supply alarm function</li> <li>• Fan and temperature alarms</li> </ul>
Maintenance	<ul style="list-style-type: none"> <li>• Debugging information output</li> <li>• Ping and Tracert</li> <li>• Remote maintenance through Telnet</li> <li>• NQA</li> <li>• 802.1ag</li> <li>• 802.3ah</li> <li>• DLDP</li> <li>• Virtual Cable Test</li> </ul>

# Appendix B Fixed security vulnerabilities

## Fixed security vulnerabilities in R6343

### **CVE-2022-0778**

A flaw was found in OpenSSL. It is possible to trigger an infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens before verification of the certificate signature, any process that parses an externally supplied certificate may be subject to a denial of service attack.



# Appendix C 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**.

---

### NOTE:

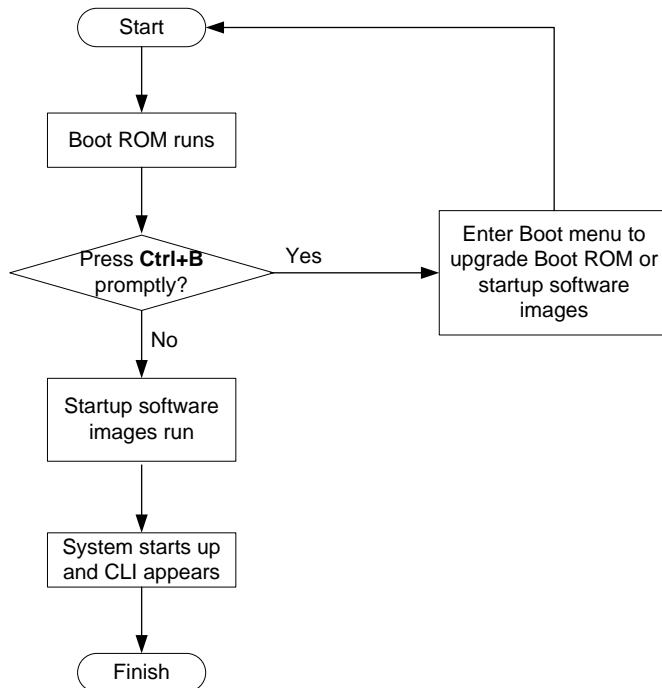
Boot ROM images are not released along with the boot images and system images. To get a version of Boot ROM image, contact the H3C technical support.

---

## 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	<ul style="list-style-type: none"> <li>Boot ROM image</li> <li>Software images</li> </ul>	<ul style="list-style-type: none"> <li>You must reboot the switch to complete the upgrade.</li> <li>This method can interrupt ongoing network services.</li> </ul>
Upgrading from the Boot menu	<ul style="list-style-type: none"> <li>Boot ROM image</li> <li>Software images</li> </ul>	<p>Use this method when the switch cannot correctly start up.</p> <p><b>⚠ CAUTION:</b></p> <p>Upgrading an IRF fabric from the CLI instead of the Boot menu.</p> <p>The Boot menu method increases the service downtime, because it requires that you upgrade the member switches one by one.</p>

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, 5140EI-CMW710-BOOT-R6367.bin and 5140EI-CMW710-SYSM-R6367.bin.

# Preparing for the upgrade

## Verifying device status

1. Verify that the system state, redundancy state, and state of each slot are stable.  

```
<Sysname> display system stable state
```

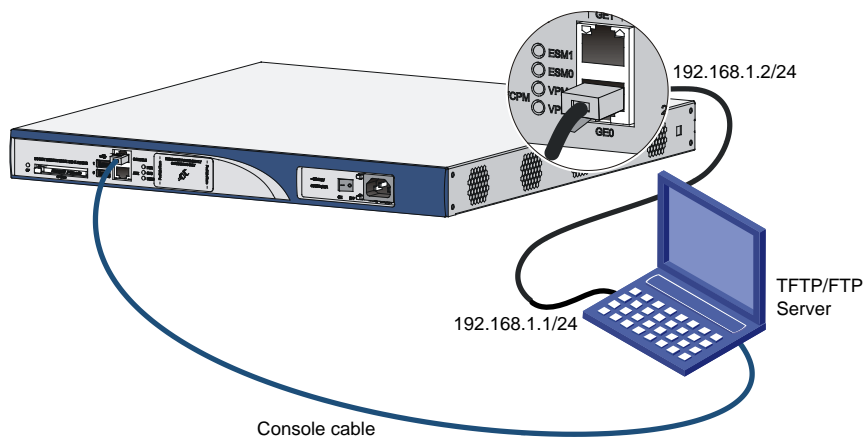
System state	:	Stable	
Redundancy state	:	No redundancy	
Slot	CPU	Role	State
1	0	Active	Stable
2. If the device is unstable, use the following commands to troubleshoot the issue:
  - Use the **display device** command to verify that the device is operating correctly.
  - Use the **display ha service-group** command to verify that bulk backup has been finished for all modules.
  - Use the **display system internal process state** command in probe view to verify that services are running correctly.
3. If a slot persists in unstable state or there are other unrecoverable issues, contact the technical support.

## Setting up the upgrade environment

Before you upgrade system software, complete the following tasks:

- Set up the upgrade environment as shown in [Figure 2](#).
- Configure routes to make sure that the router and the file server can reach each other.
- Run a TFTP or FTP server on the file server.
- Log in to the CLI of the router through the console port.
- Copy the upgrade file to the file server and correctly set the working directory on the TFTP or FTP server.
- Make sure that the upgrade has minimal impact on the network services. During the upgrade, the router cannot provide any services.

**Figure 2 Setting up the upgrade environment**



# 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 5140EI 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 drw-	-	Jan 01 2013 00:17:27	diagfile
1 drw-	-	Jan 01 2013 00:17:28	license
2 drw-	-	Jan 01 2013 00:17:27	logfile
3 drw-	-	Jan 01 2013 00:17:41	pki
4 -rw-	6161408	Jan 01 2013 00:17:27	boot.bin
5 -rw-	50729984	Jan 01 2013 00:17:27	system.bin
6 drw-	-	Jan 01 2013 00:17:27	seclog
7 drw-	-	Jan 01 2013 00:17:49	versionInfo

```
251904 KB total (192736 KB free)
```

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

```
<Sysname> dir slot2#flash:/
```

```
Directory of slot2#flash:/
```

0 drw-	-	Jan 01 2013 00:17:27	diagfile
1 drw-	-	Jan 01 2013 00:17:28	license

```

2 drw-          - Jan 01 2013 00:17:27  logfile
3 drw-          - Jan 01 2013 00:17:41  pki
4 -rw-      6161408 Jan 01 2013 00:17:27  boot.bin
5 -rw-      50729984 Jan 01 2013 00:17:27  system.bin
6 drw-          - Jan 01 2013 00:17:27  seclog
7 drw-          - Jan 01 2013 00:17:49  versionInfo

```

```
251904 KB total (192736 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
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 is Image (Binary)
```

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 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
```

```
User(1.1.1.1:(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 the file flash:/newest.ipe on slot 1.....Done.

Images in IPE:

```
boot.bin
```

```
system.bin
```

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

Add images to slot 1.

Decompressing file boot.bin to flash:/boot.bin.....Done.

Decompressing file system.bin to flash:/system.bin.....Done.

Verifying the file flash:/boot.bin on slot 1...Done.

Verifying the file flash:/system.bin on slot 1.....Done.

The images that have passed all examinations will be used as the main startup software 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 the file flash:/newest.ipe on slot 2.....Done.

Images in IPE:

```

boot.bin
system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 2.
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to flash:/system.bin.....Done.
Verifying the file flash:/boot.bin on slot 2...Done.
Verifying the file flash:/system.bin on slot 2.....Done.
The images that have passed all examinations will be used as the main startup software
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 9](#).

**Table 9 Minimum free storage space requirements**

Upgraded images	Minimum free storage space requirements
Comware images	Two times the size of the Comware upgrade package file.

Upgraded images	Minimum free storage space requirements
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
Booting Normal Extend BootWare....

*****
*
*          HPE 5140 24G PoE+ 4SFP+ EI Sw BOOTROM, Version 158          *
*
*****

Copyright (c) 2010-2024 Hewlett Packard Enterprise Development LP

Creation Date       : Mar 13 2023, 17:35:17
CPU Clock Speed    : 800MHz
Memory Size        : 512MB
Flash Size         : 256MB
CPLD Version       : 001
PCB Version        : Ver.A
Mac Address        : aa1122334455
Press Ctrl+B to access EXTENDED BOOT MENU...1
```

Press one of the shortcut key combinations at prompt.

**Table 10 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.

# 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 11](#)). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE FlexNetwork 5140 EI Switch Series Configuration Guides-R63xx*.

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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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

**Table 11 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	<ul style="list-style-type: none"><li>Specify the main and backup software image file for the next startup.</li><li>Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.</li></ul>
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.

Option	Tasks
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 <a href="#">Table 12</a> .
Ctrl+Y: Change Work Mode	Change Work Mode.
Ctrl+C: Display Copyright	Display the copyright statement.

**Table 12 EXTENDED ASSISTANT menu options**

Option	Task
1. Display Memory	Display data in the memory.
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 13 TFTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.ipe</b> ).
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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright
```

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 14 FTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.ipe</b> ).

Item	Description
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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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 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
```

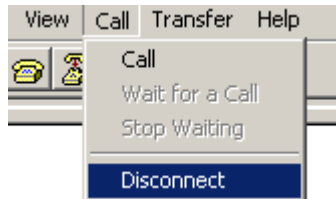
```
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
```



Press enter key when ready

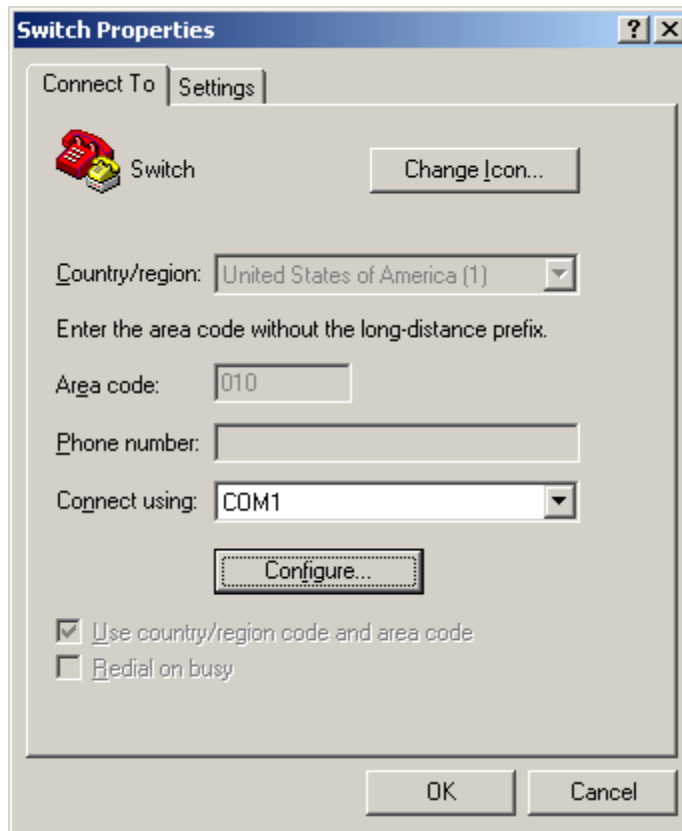
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
  - a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

**Figure 3 Disconnecting the terminal from the switch**



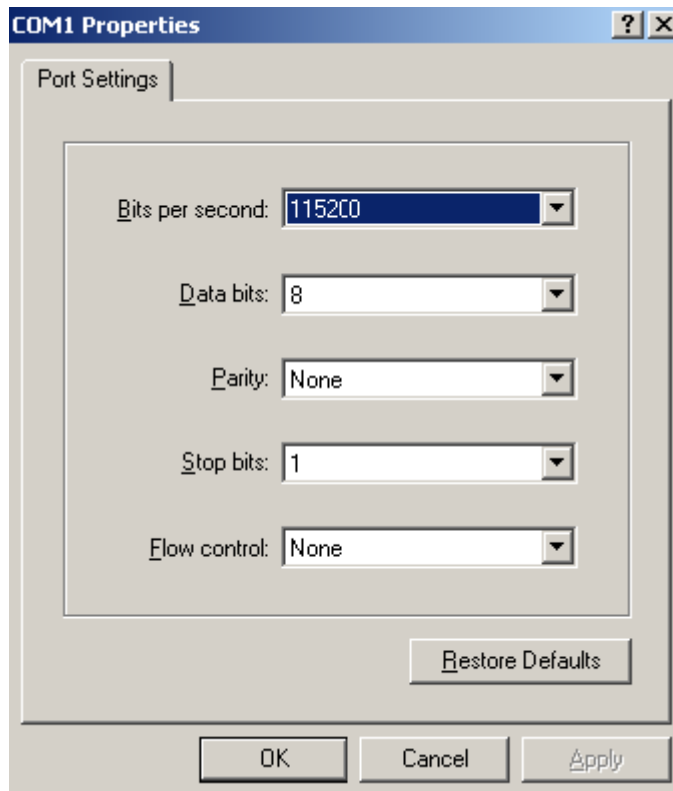
- b. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

**Figure 4 Properties dialog box**



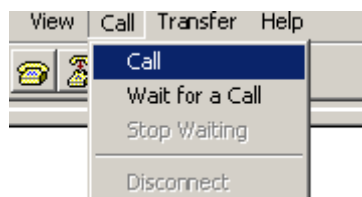
- c. Select **115200** from the **Bits per second** list and click **OK**.

**Figure 5 Modifying the baud rate**



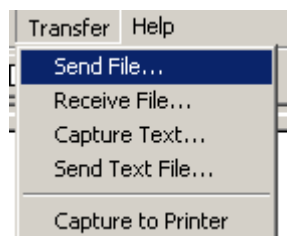
- d. Select **Call** > **Call** to reestablish the connection.

**Figure 6 Reestablishing the connection**



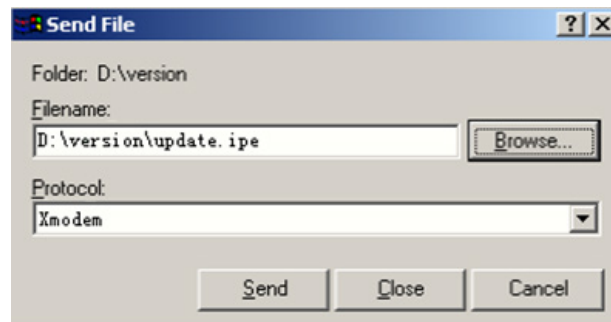
5. Press **Enter**. The following prompt appears:  
Are you sure to download file to flash? Yes or No (Y/N):Y
6. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)  
Now please start transfer file with XMODEM protocol  
If you want to exit, Press <Ctrl+X>  
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCCCC
7. Select **Transfer** > **Send File** in the HyperTerminal window.

**Figure 7 Transfer menu**



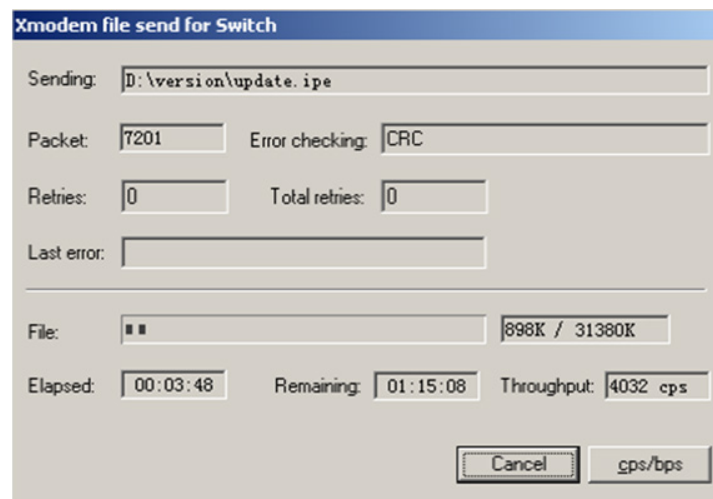
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

**Figure 8 File transmission dialog box**



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

**Figure 9 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 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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright
```

```
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 15 TFTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.btm</b> ).
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 16 FTP parameter description**

Item	Description
Load File Name	Name of the file to download (for example, <b>update.btm</b> ).
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

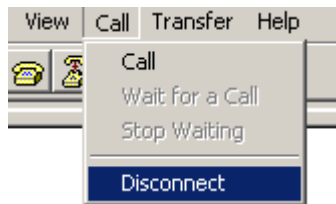
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

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.

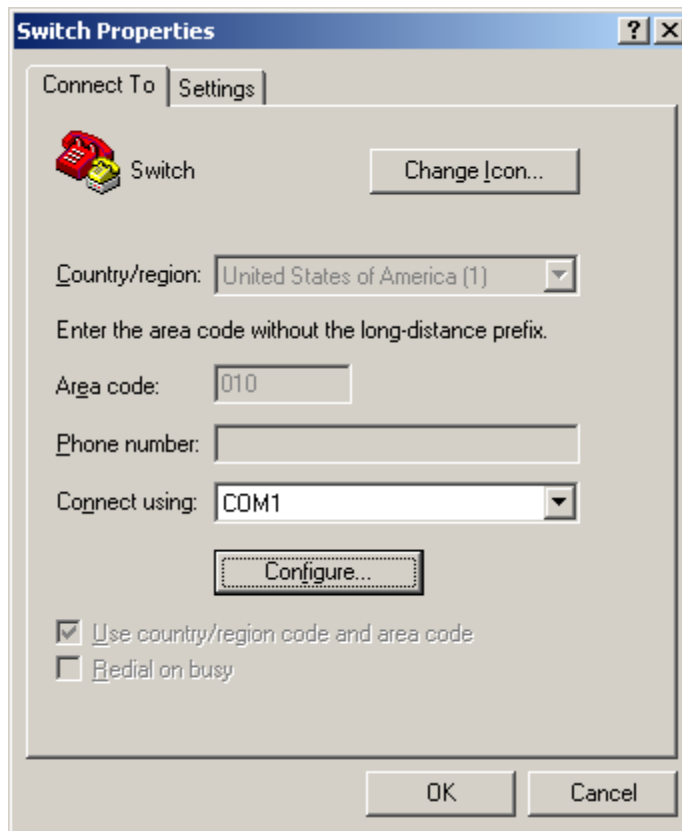
- a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

**Figure 10 Disconnecting the terminal from the switch**



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

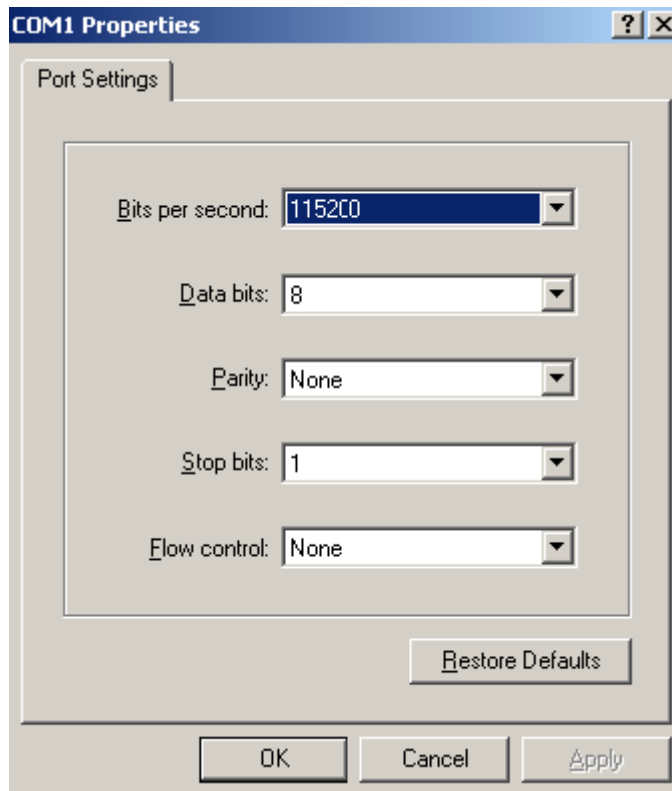
**Figure 11 Properties dialog box**



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

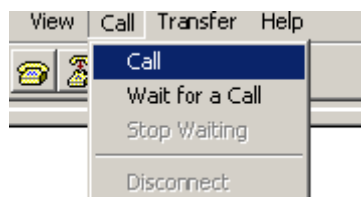


**Figure 12 Modifying the baud rate**



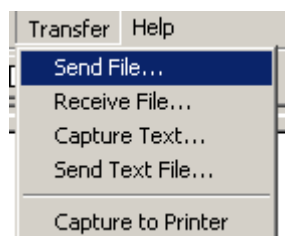
- d. Select **Call > Call** to reestablish the connection.

**Figure 13 Reestablishing the connection**



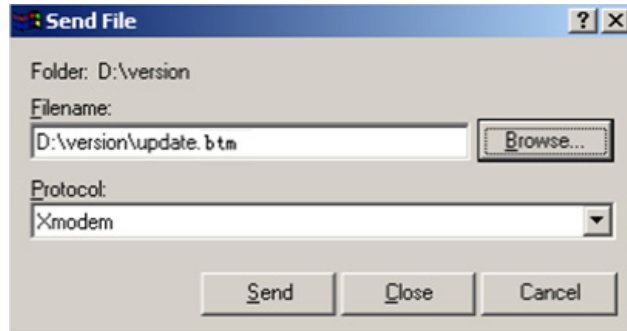
6. Press **Enter** to start downloading the file.  
Now please start transfer file with XMODEM protocol  
If you want to exit, Press <Ctrl+X>  
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
7. Select **Transfer > Send File** in the HyperTerminal window.

**Figure 14 Transfer menu**



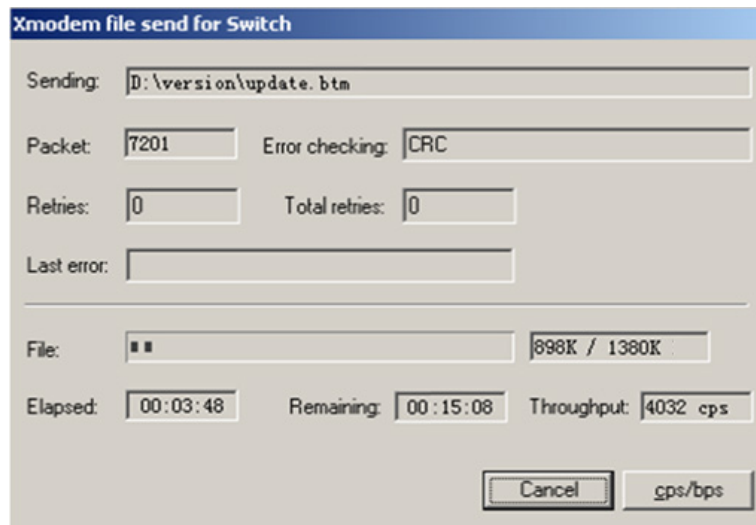
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

Figure 15 File transmission dialog box



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

Figure 16 File transfer progress



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

```
Loading ...CCCCCCCCCCCCCCCC ...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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright
```

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
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

```

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.
- 8.



**Hewlett Packard**  
Enterprise

# HPE 5140\_EI-CMW710-R6367 Release Notes

## Software Feature Changes

The information in this document is subject to change without notice.

© Copyright 2024 Hewlett Packard Enterprise Development LP

# Contents

|                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------|----|
| R6367 .....                                                                                                         | 1  |
| New Feature: Enabling port security unified secure MAC address control for access users.....                        | 1  |
| Enabling port security unified secure MAC address control for access users .....                                    | 1  |
| Command reference .....                                                                                             | 2  |
| New command: port-security user-mac control enable.....                                                             | 2  |
| Modified command: display port-security mac-address security.....                                                   | 3  |
| Modified feature: Configuring the padding mode and padding format for the Circuit ID sub-option .....               | 4  |
| Feature change description.....                                                                                     | 4  |
| Command changes .....                                                                                               | 4  |
| Modified command: dhcp relay information circuit-id .....                                                           | 4  |
| Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option .....                | 5  |
| Feature change description.....                                                                                     | 5  |
| Command changes .....                                                                                               | 5  |
| Modified command: dhcp relay information remote-id .....                                                            | 5  |
| Release 6363 .....                                                                                                  | 6  |
| New feature: Enabling port selection preemption on an aggregate interface ..                                        | 6  |
| Enabling port selection preemption on an aggregate interface.....                                                   | 6  |
| Command reference .....                                                                                             | 7  |
| lACP preempt delay.....                                                                                             | 7  |
| lACP preempt enable.....                                                                                            | 7  |
| New feature: Configuring an interface as an uplink interface to disable it from learning ARP snooping entries ..... | 8  |
| Configuring an interface as an uplink interface to disable it from learning ARP snooping entries .....              | 8  |
| Command reference .....                                                                                             | 9  |
| arp snooping uplink.....                                                                                            | 9  |
| New feature: Configuring spanning tree blackhole detection .....                                                    | 10 |
| Configuring spanning tree blackhole detection .....                                                                 | 10 |
| Command changes .....                                                                                               | 12 |
| display stp blackhole-detection blocked-port .....                                                                  | 12 |
| stp blackhole-detection enable.....                                                                                 | 13 |
| stp global blackhole-detection enable .....                                                                         | 14 |
| stp global blackhole-detection rx-bpdu timeout.....                                                                 | 16 |
| stp global timer blackhole-detection-interval .....                                                                 | 17 |
| stp global timer rx-blackhole-timeout .....                                                                         | 18 |
| stp timer blackhole-detection-interval.....                                                                         | 19 |
| stp timer rx-blackhole-timeout .....                                                                                | 20 |
| New feature: LLDP back hole detection .....                                                                         | 21 |
| Configuring LLDP black hole detection .....                                                                         | 21 |
| Command reference .....                                                                                             | 24 |
| lldp blackhole-detection enable.....                                                                                | 24 |
| lldp global blackhole-detection enable .....                                                                        | 26 |
| lldp global blackhole-detection rx-lldpdu timeout .....                                                             | 28 |
| lldp global timer blackhole-detection-interval .....                                                                | 29 |
| lldp global timer rx-blackhole-timeout.....                                                                         | 30 |



|                                                                                                                                               |           |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| lldp timer blackhole-detection-interval .....                                                                                                 | 31        |
| lldp timer rx-blackhole-timeout .....                                                                                                         | 32        |
| <b>New feature: LLDP cross-domain detection .....</b>                                                                                         | <b>33</b> |
| Configuring LLDP cross-domain detection .....                                                                                                 | 33        |
| Command reference .....                                                                                                                       | 35        |
| lldp cross-domain-detection .....                                                                                                             | 35        |
| lldp cross-domain-detection domain-id .....                                                                                                   | 36        |
| lldp global cross-domain-detection enable .....                                                                                               | 38        |
| <b>New feature: Using the subscriber ID as the client ID in all received DHCP requests .....</b>                                              | <b>40</b> |
| Using the subscriber ID as the client ID in all received DHCP requests .....                                                                  | 40        |
| Command reference .....                                                                                                                       | 41        |
| dhcp server subscriber-id replace client-id .....                                                                                             | 41        |
| dhcp server subscriber-id replace client-id global .....                                                                                      | 42        |
| dhcp server subscriber-id interface-name .....                                                                                                | 43        |
| <b>New feature: Configuring resource monitoring .....</b>                                                                                     | <b>44</b> |
| Configuring resource monitoring .....                                                                                                         | 44        |
| Command reference .....                                                                                                                       | 45        |
| display resource-monitor .....                                                                                                                | 45        |
| resource-monitor minor resend enable .....                                                                                                    | 46        |
| resource-monitor output .....                                                                                                                 | 47        |
| resource-monitor resource .....                                                                                                               | 47        |
| <b>New feature: Sending EAP-Success packets upon successful authorization in 802.1X .....</b>                                                 | <b>49</b> |
| Sending EAP-Success packets upon successful authorization .....                                                                               | 49        |
| Command reference .....                                                                                                                       | 50        |
| dot1x eap-success post-authorization .....                                                                                                    | 50        |
| <b>Modified feature: Support for specifying a custom hexadecimal string as the content of the Remote ID sub-option .....</b>                  | <b>51</b> |
| Feature change description .....                                                                                                              | 51        |
| Command changes .....                                                                                                                         | 51        |
| Modified command: dhcp snooping information remote-id .....                                                                                   | 51        |
| Modified command: dhcp relay information remote-id .....                                                                                      | 51        |
| <b>Modified feature: Support for specifying a custom ASCII string as the client ID of a static binding .....</b>                              | <b>52</b> |
| Feature change description .....                                                                                                              | 52        |
| Modified command: static-bind .....                                                                                                           | 52        |
| <b>Release 6351P02 .....</b>                                                                                                                  | <b>54</b> |
| <b>Release 6351 .....</b>                                                                                                                     | <b>55</b> |
| <b>New feature: Advertising proprietary TLVs on an interface .....</b>                                                                        | <b>56</b> |
| Advertising proprietary TLVs on an interface .....                                                                                            | 56        |
| Command reference .....                                                                                                                       | 56        |
| lldp tlv-enable private-tlv .....                                                                                                             | 56        |
| <b>New feature: Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection .....</b> | <b>57</b> |
| Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection .....                     | 57        |
| Command reference .....                                                                                                                       | 57        |
| lacp select speed .....                                                                                                                       | 57        |

|                                                                                                                   |           |
|-------------------------------------------------------------------------------------------------------------------|-----------|
| <b>New feature: Loopback test on an interface.....</b>                                                            | <b>58</b> |
| Performing a loopback test on an interface .....                                                                  | 58        |
| About this task.....                                                                                              | 58        |
| Restrictions and guidelines .....                                                                                 | 59        |
| Procedure.....                                                                                                    | 59        |
| Command reference .....                                                                                           | 59        |
| New command: loopback-test.....                                                                                   | 59        |
| <b>New feature: Configuring disk usage monitoring.....</b>                                                        | <b>59</b> |
| Command changes .....                                                                                             | 60        |
| monitor disk-usage disk .....                                                                                     | 60        |
| monitor disk-usage interval .....                                                                                 | 61        |
| <b>New feature: Enabling the portal fail-permit feature for portal Web servers ·</b>                              | <b>61</b> |
| Enabling the portal fail-permit feature for portal Web servers.....                                               | 61        |
| Command reference .....                                                                                           | 62        |
| portal fail-permit web-server.....                                                                                | 62        |
| <b>New feature: Configuring packet detection for 802.1X authentication .....</b>                                  | <b>63</b> |
| Configuring packet detection for 802.1X authentication .....                                                      | 63        |
| Command reference .....                                                                                           | 64        |
| New command: dot1x packet-detect enable .....                                                                     | 64        |
| New command: dot1x packet-detect retry.....                                                                       | 65        |
| Modified command: display dot1x connection .....                                                                  | 66        |
| <b>New feature: Configuring packet detection for MAC authentication .....</b>                                     | <b>67</b> |
| Configuring packet detection for MAC authentication.....                                                          | 67        |
| Command reference .....                                                                                           | 69        |
| New command: mac-authentication packet-detect enable .....                                                        | 69        |
| New command: mac-authentication packet-detect retry .....                                                         | 70        |
| Modified command: display mac-authentication connection.....                                                      | 70        |
| <b>New feature: Specifying an IP address and mask for calculating the source IP of ARP detection packets.....</b> | <b>71</b> |
| Specifying an IP address and mask for calculating the source IP of ARP detection packets.....                     | 71        |
| Command reference .....                                                                                           | 72        |
| port-security packet-detect arp-source-ip factor.....                                                             | 72        |
| <b>New feature: Associating PoE with Track .....</b>                                                              | <b>73</b> |
| Associating PoE with Track.....                                                                                   | 73        |
| Command reference .....                                                                                           | 74        |
| poe track .....                                                                                                   | 74        |
| <b>New feature: many-to-one VLAN mapping.....</b>                                                                 | <b>75</b> |
| Configuring many-to-one VLAN mapping .....                                                                        | 75        |
| About many-to-one VLAN mapping .....                                                                              | 75        |
| About many-to-one VLAN mapping .....                                                                              | 75        |
| Command reference .....                                                                                           | 76        |
| vlan mapping uni .....                                                                                            | 76        |
| <b>New feature: Disabling receiving a specific type of ICMP messages .....</b>                                    | <b>77</b> |
| Disabling receiving a specific type of ICMP messages.....                                                         | 77        |
| Command reference .....                                                                                           | 78        |
| ip icmp receive enable .....                                                                                      | 78        |
| <b>New feature: Disabling sending a specific type of ICMP messages .....</b>                                      | <b>79</b> |
| Disabling sending a specific type of ICMP messages.....                                                           | 79        |
| Command reference .....                                                                                           | 80        |
| ip icmp send enable .....                                                                                         | 80        |

|                                                                                                        |           |
|--------------------------------------------------------------------------------------------------------|-----------|
| <b>New feature: MAC swap loopback test configuration .....</b>                                         | <b>82</b> |
| Configuring a MAC swap loopback test .....                                                             | 82        |
| Command reference .....                                                                                | 82        |
| loopback local swap-mac .....                                                                          | 82        |
| loopback remote swap-mac .....                                                                         | 84        |
| loopback swap-mac .....                                                                                | 85        |
| display loopback swap-mac information .....                                                            | 85        |
| <b>New feature: Configuring the TMPDO for the MPS .....</b>                                            | <b>87</b> |
| Configuring the TMPDO for the MPS .....                                                                | 87        |
| Command reference .....                                                                                | 87        |
| poe mps .....                                                                                          | 87        |
| <b>New feature: Configuring port collaboration .....</b>                                               | <b>88</b> |
| Configuring port collaboration .....                                                                   | 88        |
| Command reference .....                                                                                | 89        |
| cfd port-trigger .....                                                                                 | 89        |
| <b>New feature: Disabling PoE power supply on shutdown interfaces .....</b>                            | <b>90</b> |
| Disabling PoE power supply on shutdown interfaces .....                                                | 90        |
| Command reference .....                                                                                | 91        |
| poe track-shutdown .....                                                                               | 91        |
| <b>New feature: Configuring PoE delay .....</b>                                                        | <b>91</b> |
| Configuring PoE delay .....                                                                            | 91        |
| Command reference .....                                                                                | 92        |
| poe power-delay .....                                                                                  | 92        |
| <b>New feature: Setting the PoE guard band .....</b>                                                   | <b>93</b> |
| Setting the PoE guard band .....                                                                       | 93        |
| Command reference .....                                                                                | 93        |
| poe guard-band .....                                                                                   | 93        |
| <b>New feature: Configuring a PD disconnection detection mode .....</b>                                | <b>94</b> |
| Configuring a PD disconnection detection mode .....                                                    | 94        |
| Command reference .....                                                                                | 94        |
| poe disconnect .....                                                                                   | 94        |
| <b>New feature: Ignoring the PD power class .....</b>                                                  | <b>95</b> |
| Ignoring the PD power class .....                                                                      | 95        |
| Command reference .....                                                                                | 96        |
| poe class-detect ignore .....                                                                          | 96        |
| <b>Modified feature: Applying a portal Web server to an interface .....</b>                            | <b>96</b> |
| Feature change description .....                                                                       | 96        |
| Command changes .....                                                                                  | 97        |
| Modified command: portal apply web-server .....                                                        | 97        |
| <b>Modified feature: Displaying portal configuration and running information on an interface .....</b> | <b>97</b> |
| Feature change description .....                                                                       | 97        |
| Command changes .....                                                                                  | 97        |
| Modified command: display portal .....                                                                 | 97        |
| <b>Modified feature: Display power supply information .....</b>                                        | <b>99</b> |
| Feature change description .....                                                                       | 99        |
| Command changes .....                                                                                  | 99        |
| Modified command: display power .....                                                                  | 99        |

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| Modified feature: Configuring the padding mode and padding format for the Circuit ID sub-option in VLAN view ..... | 99  |
| Feature change description.....                                                                                    | 99  |
| Command changes .....                                                                                              | 100 |
| Modified command: dhcp snooping information circuit-id .....                                                       | 100 |
| Modified feature: Enabling DHCP snooping to support Option 82 in VLAN view .....                                   | 100 |
| Feature change description.....                                                                                    | 100 |
| Command changes .....                                                                                              | 100 |
| Modified command: dhcp snooping information enable.....                                                            | 100 |
| Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option in VLAN view .....  | 101 |
| Feature change description.....                                                                                    | 101 |
| Command changes .....                                                                                              | 101 |
| Modified command: dhcp snooping information remote-id .....                                                        | 101 |
| Modified feature: Configuring the Option 82 handling strategy for DHCP request messages in VLAN view .....         | 101 |
| Feature change description.....                                                                                    | 101 |
| Command changes .....                                                                                              | 102 |
| Modified command: dhcp snooping information strategy.....                                                          | 102 |
| Modified feature: Configuring the padding mode for the Vendor-Specific sub-option in VLAN view.....                | 102 |
| Feature change description.....                                                                                    | 102 |
| Command changes .....                                                                                              | 102 |
| Modified command: dhcp snooping information vendor-specific .....                                                  | 102 |
| Modified feature: Changing the default settings for outputting port state transition information .....             | 103 |
| Feature change description.....                                                                                    | 103 |
| Command changes .....                                                                                              | 103 |
| Modified command: stp port-log.....                                                                                | 103 |
| Modified feature: Support of 10G fiber ports for 2.5G transceiver modules                                          | 103 |
| Feature change description.....                                                                                    | 103 |
| Command changes .....                                                                                              | 103 |
| Modified command: speed .....                                                                                      | 103 |
| Modified feature: PD detection mode.....                                                                           | 104 |
| Feature change description.....                                                                                    | 104 |
| Command changes .....                                                                                              | 104 |
| Modified command: poe detection-mode .....                                                                         | 104 |
| Modified feature: Enabling recording user IP address conflicts .....                                               | 104 |
| Feature change description.....                                                                                    | 104 |
| Command changes .....                                                                                              | 104 |
| Modified command: arp user-ip-conflict record enable .....                                                         | 104 |
| Modified feature: Enabling IP conflict notification .....                                                          | 105 |
| Feature change description.....                                                                                    | 105 |
| Command changes .....                                                                                              | 105 |
| Modified command: arp ip-conflict log prompt .....                                                                 | 105 |
| Modified feature: Testing the cable connection of an Ethernet interface ....                                       | 105 |
| Feature change description.....                                                                                    | 105 |

|                                                                                                                         |            |
|-------------------------------------------------------------------------------------------------------------------------|------------|
| Modified command: virtual-cable-test .....                                                                              | 105        |
| New command: display virtual-cable-test.....                                                                            | 106        |
| reset interface virtual-cable-test.....                                                                                 | 108        |
| <b>Modified feature: Allowing inrush currents of PDs.....</b>                                                           | <b>108</b> |
| Feature change description.....                                                                                         | 108        |
| Command changes .....                                                                                                   | 108        |
| Modified command: poe high-inrush enable .....                                                                          | 108        |
| <b>Release 6343P09 .....</b>                                                                                            | <b>110</b> |
| <b>Modified feature: Factory defaults change for console login and password control settings .....</b>                  | <b>110</b> |
| Feature change description.....                                                                                         | 110        |
| <b>Command changes.....</b>                                                                                             | <b>111</b> |
| <b>Release 6343 .....</b>                                                                                               | <b>112</b> |
| <b>New feature: Configuring interface alarm functions.....</b>                                                          | <b>112</b> |
| Command changes .....                                                                                                   | 113        |
| ifmonitor input-error.....                                                                                              | 113        |
| ifmonitor output-error.....                                                                                             | 114        |
| port ifmonitor input-error.....                                                                                         | 115        |
| port ifmonitor output-error .....                                                                                       | 116        |
| Modified command: snmp-agent trap enable ifmonitor .....                                                                | 117        |
| <b>New feature: Configuring the aging timer for temporary MAC address entries for Web authentication.....</b>           | <b>118</b> |
| Command reference .....                                                                                                 | 119        |
| New command: web-auth timer temp-entry-aging .....                                                                      | 119        |
| Modified command: display web-auth.....                                                                                 | 120        |
| <b>Modified feature: Displaying the running configuration.....</b>                                                      | <b>120</b> |
| Feature change description.....                                                                                         | 120        |
| Command changes .....                                                                                                   | 120        |
| Modified command: display current-configuration.....                                                                    | 120        |
| <b>Modified feature: Displaying the running configuration in current view .....</b>                                     | <b>121</b> |
| Feature change description.....                                                                                         | 121        |
| Command changes .....                                                                                                   | 121        |
| Modified command: display this .....                                                                                    | 121        |
| <b>Modified feature: 802.1X periodic reauthentication timer .....</b>                                                   | <b>121</b> |
| Feature change description.....                                                                                         | 121        |
| Command changes .....                                                                                                   | 121        |
| Modified command: dot1x timer reauth-period (system view).....                                                          | 121        |
| Modified command: dot1x timer reauth-period (interface view) .....                                                      | 122        |
| <b>Modified feature: Periodic MAC reauthentication timer .....</b>                                                      | <b>122</b> |
| Feature change description.....                                                                                         | 122        |
| Command changes .....                                                                                                   | 122        |
| Modified command: mac-authentication timer (system view) .....                                                          | 122        |
| Modified command: mac-authentication timer (interface view) .....                                                       | 122        |
| <b>Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option of Option 82.....</b> | <b>123</b> |
| Feature change description.....                                                                                         | 123        |
| Command changes .....                                                                                                   | 123        |
| Modified command: dhcp relay information remote-id .....                                                                | 123        |

|                                                                                              |            |
|----------------------------------------------------------------------------------------------|------------|
| <b>Modified feature: Configuring gRPC collectors .....</b>                                   | <b>123</b> |
| Feature change description.....                                                              | 123        |
| Command changes .....                                                                        | 124        |
| New command: domain-name .....                                                               | 124        |
| New command: ipv6 domain-name.....                                                           | 125        |
| Modified command: display grpc.....                                                          | 126        |
| <b>Modified feature: Displaying detailed information about 802.1X online users .....</b>     | <b>127</b> |
| Feature change description.....                                                              | 127        |
| Command changes .....                                                                        | 127        |
| Modified command: display dot1x connection .....                                             | 127        |
| <b>Release 6337P01 .....</b>                                                                 | <b>129</b> |
| <b>New feature: Configuring SmartMC .....</b>                                                | <b>129</b> |
| About SmartMC.....                                                                           | 129        |
| SmartMC network framework.....                                                               | 129        |
| SmartMC network establishment .....                                                          | 130        |
| SmartMC features .....                                                                       | 131        |
| Restrictions: Hardware compatibility with SmartMC .....                                      | 134        |
| Restrictions and guidelines: SmartMC configuration .....                                     | 134        |
| SmartMC tasks at a glance .....                                                              | 134        |
| Prerequisites for SmartMC.....                                                               | 135        |
| Enabling SmartMC .....                                                                       | 135        |
| Setting the file server information .....                                                    | 136        |
| Configuring an outgoing interface for the SmartMC network .....                              | 137        |
| Enabling automatic Ethernet link aggregation .....                                           | 137        |
| Modifying the password of the default user for members .....                                 | 137        |
| Creating a SmartMC group .....                                                               | 138        |
| Creating a VLAN for members.....                                                             | 138        |
| Deploying a batch file to members.....                                                       | 139        |
| Configuring a batch file for ports connecting APs or IP phones.....                          | 139        |
| Backing up configuration files .....                                                         | 139        |
| Configuring resource monitoring.....                                                         | 140        |
| Upgrading the startup software and configuration file on members.....                        | 141        |
| About upgrading the startup software and configuration file on members .....                 | 141        |
| Restrictions and guidelines for startup software and configuration file upgrade .....        | 141        |
| Prerequisites .....                                                                          | 141        |
| Upgrading the startup software and configuration file on members.....                        | 141        |
| Upgrading the startup software and configuration file on all members in SmartMC groups ..... | 142        |
| Managing the network topology .....                                                          | 143        |
| Refreshing the network topology.....                                                         | 143        |
| Saving the network topology.....                                                             | 144        |
| Replacing faulty members.....                                                                | 144        |
| Display and maintenance commands for SmartMC.....                                            | 145        |
| SmartMC configuration examples .....                                                         | 145        |
| Example: Configuring SmartMC.....                                                            | 145        |
| Command reference .....                                                                      | 148        |
| boot-loader file .....                                                                       | 148        |
| create batch-file.....                                                                       | 149        |
| display smartmc backup configuration status .....                                            | 150        |
| display smartmc batch-file status .....                                                      | 151        |
| display smartmc configuration.....                                                           | 152        |
| display smartmc device-link .....                                                            | 154        |
| display smartmc group .....                                                                  | 154        |
| display smartmc replace status.....                                                          | 156        |
| display smartmc resource-monitor .....                                                       | 156        |
| display smartmc resource-monitor configuration .....                                         | 157        |
| display smartmc tc .....                                                                     | 158        |

|                                                                                           |            |
|-------------------------------------------------------------------------------------------|------------|
| display smartmc tc log buffer .....                                                       | 160        |
| display smartmc tc log restart .....                                                      | 161        |
| display smartmc upgrade status .....                                                      | 162        |
| display smartmc vlan .....                                                                | 163        |
| match .....                                                                               | 164        |
| smartmc auto-link-aggregation enable .....                                                | 164        |
| smartmc auto-replace enable .....                                                         | 165        |
| smartmc backup configuration .....                                                        | 166        |
| smartmc backup configuration max-number .....                                             | 166        |
| smartmc backup configuration interval .....                                               | 167        |
| smartmc batch-file apply .....                                                            | 168        |
| smartmc batch-file deploy .....                                                           | 169        |
| smartmc batch-file-apply enable .....                                                     | 169        |
| smartmc enable .....                                                                      | 170        |
| smartmc { ftp-server   sftp-server } .....                                                | 171        |
| smartmc group .....                                                                       | 172        |
| smartmc outbound .....                                                                    | 173        |
| smartmc resource-monitor .....                                                            | 173        |
| smartmc resource-monitor interval .....                                                   | 175        |
| smartmc resource-monitor max-age .....                                                    | 175        |
| smartmc replace .....                                                                     | 176        |
| smartmc tc boot-loader .....                                                              | 177        |
| smartmc tc device-type .....                                                              | 177        |
| smartmc tc password .....                                                                 | 178        |
| smartmc tc startup-configuration .....                                                    | 179        |
| smartmc topology-refresh .....                                                            | 179        |
| smartmc topology-refresh interval .....                                                   | 180        |
| smartmc topology-save .....                                                               | 180        |
| smartmc upgrade boot-loader .....                                                         | 181        |
| smartmc upgrade startup-configuration .....                                               | 182        |
| smartmc vlan .....                                                                        | 183        |
| startup-configuration .....                                                               | 184        |
| <b>New feature: Configuring interface alarm functions .....</b>                           | <b>186</b> |
| Configuring interface alarm functions .....                                               | 186        |
| Command reference .....                                                                   | 187        |
| ifmonitor crc-error .....                                                                 | 187        |
| port ifmonitor crc-error .....                                                            | 188        |
| snmp-agent trap enable ifmonitor .....                                                    | 189        |
| <b>New feature: Configuring Option 60 for DHCP requests .....</b>                         | <b>189</b> |
| Configuring Option 60 for DHCP requests .....                                             | 189        |
| Command reference .....                                                                   | 190        |
| dhcp client class-id .....                                                                | 190        |
| <b>New feature: Configuring the type of port ID TLVs advertised by LLDP .....</b>         | <b>191</b> |
| Configuring the type of port ID TLVs advertised by LLDP .....                             | 191        |
| Command reference .....                                                                   | 192        |
| lldp global tlv-config basic-tlv port-id .....                                            | 192        |
| lldp tlv-config basic-tlv port-id .....                                                   | 192        |
| <b>New feature: Enabling displaying LLDP local information about all interfaces .....</b> | <b>193</b> |
| Enabling displaying LLDP local information about all interfaces .....                     | 193        |
| Command reference .....                                                                   | 194        |
| lldp local-information all-interface .....                                                | 194        |
| <b>New feature: PoE forced power supply .....</b>                                         | <b>195</b> |
| Enabling PoE forced power supply .....                                                    | 195        |
| Command reference .....                                                                   | 195        |
| poe force-power .....                                                                     | 195        |

|                                                                                                              |            |
|--------------------------------------------------------------------------------------------------------------|------------|
| Command changes .....                                                                                        | 196        |
| Modified command: display poe pse .....                                                                      | 196        |
| <b>New feature: Interval at which the SNMP module examines the system configuration for changes .....</b>    | <b>197</b> |
| Setting the interval at which the SNMP module examines the system configuration for changes .....            | 197        |
| Command reference .....                                                                                      | 197        |
| snmp-agent configuration-examine interval .....                                                              | 197        |
| <b>New feature: Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users .....</b> | <b>198</b> |
| Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users .....                     | 198        |
| dot1x { ip-verify-source   ipv6-verify-source } enable .....                                                 | 199        |
| <b>New feature: Automated IPv6 underlay network deployment for VCF fabric .....</b>                          | <b>199</b> |
| About automated IPv6 underlay network deployment .....                                                       | 199        |
| Command reference .....                                                                                      | 200        |
| <b>Modified feature: Setting the port status detection timer .....</b>                                       | <b>200</b> |
| Feature change description .....                                                                             | 200        |
| Command changes .....                                                                                        | 200        |
| Modified command: shutdown-interval .....                                                                    | 200        |
| <b>Modified feature: 802.1X EAD assistant .....</b>                                                          | <b>200</b> |
| Feature change description .....                                                                             | 200        |
| Command changes .....                                                                                        | 200        |
| New command: dot1x ead-assistant permit authentication-escape .....                                          | 200        |
| <b>Modified feature: Displaying information about online 802.1X users .....</b>                              | <b>201</b> |
| Feature change description .....                                                                             | 201        |
| Command changes .....                                                                                        | 201        |
| Modified command: display dot1x connection .....                                                             | 201        |
| <b>Modified feature: Displaying information about online MAC authentication users .....</b>                  | <b>202</b> |
| Feature change description .....                                                                             | 202        |
| Command changes .....                                                                                        | 202        |
| Modified command: display mac-authentication connection .....                                                | 202        |
| <b>Modified feature: L2PT for CFD .....</b>                                                                  | <b>203</b> |
| Feature change description .....                                                                             | 203        |
| Command changes .....                                                                                        | 203        |
| Modified command: l2protocol type tunnel-dmac .....                                                          | 203        |
| Modified command: l2protocol tunnel dot1q .....                                                              | 204        |
| Modified command: display l2protocol statistics .....                                                        | 205        |
| <b>Release 6330 .....</b>                                                                                    | <b>207</b> |
| <b>New feature: Enabling fast PoE for a PSE .....</b>                                                        | <b>207</b> |
| Enabling fast PoE for a PSE .....                                                                            | 207        |
| Command reference .....                                                                                      | 207        |
| poe fast-on enable .....                                                                                     | 207        |
| <b>Modified feature: L2PT for CFD and DTP .....</b>                                                          | <b>208</b> |
| Feature change description .....                                                                             | 208        |
| Command changes .....                                                                                        | 208        |
| New command: l2protocol type tunnel-dmac .....                                                               | 208        |
| Modified command: l2protocol tunnel dot1q .....                                                              | 209        |
| Modified command: display l2protocol statistics .....                                                        | 210        |



|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| Modified feature: Displaying information about online 802.1X users .....               | 211 |
| Feature change description.....                                                        | 211 |
| Command changes .....                                                                  | 211 |
| Modified command: display dot1x connection .....                                       | 211 |
| Modified feature: Displaying information about online MAC authentication<br>users..... | 212 |
| Feature change description.....                                                        | 212 |
| Command changes .....                                                                  | 212 |
| Modified command: display mac-authentication connection.....                           | 212 |

# R6367

This release has the following changes:

- **New Feature:** Enabling port security unified secure MAC address control for access users
- **Modified feature:** Configuring the padding mode and padding format for the Circuit ID sub-option
- **Modified feature:** Configuring the padding mode and padding format for the Remote ID sub-option

## New Feature: Enabling port security unified secure MAC address control for access users

### Enabling port security unified secure MAC address control for access users

#### About this feature

By default, only the MAC addresses manually configured or automatically learned in the port security autoLearn mode are considered secure MAC addresses and are subject to related security features. To enhance network access security, the device now supports unified secure MAC management for various access users on a port.

With this feature enabled on a port, the MAC addresses of 802.1X authentication users, MAC authentication users, Web authentication users, and voice VLAN users who have successfully authenticated on the port will be added to the secure MAC table and controlled by related secure MAC functions. For example, the maximum number of secure MAC addresses on the port can be deleted using the **undo port-security mac-address security sticky** command, and support for intrusion detection on the port.

For successfully authenticated 802.1X, MAC authentication, and Web authentication users and voice VLAN users, their secure MAC addresses are sticky MAC addresses. You can convert them to dynamic secure MAC addresses by using the **port-security mac-address dynamic** command.

In contrast to sticky MAC entries generated in autoLearn mode, the sticky MAC entries for authenticated users and voice VLAN users do not age while they are online. These entries are only affected by timing and traffic aging mechanisms after the users go offline.

#### Restrictions and guidelines

Before configuring this feature, you must first set the maximum number of secure MAC addresses allowed on a port by executing the **port-security max-mac-count** command in interface view. After this feature is configured, you cannot change the limit on the number of secure MAC addresses on a port.

This feature and the autoLearn mode are mutually exclusive.

When the **dot1x port-method portbased** command or **mac-authentication host-mode multi-vlan** command is configured on a port, only the MAC address of the first authenticated user is added as a secure MAC address entry.

#### Procedure

1. Enter system view.

- system-view**
  - 2. Enter interface view.  
**interface** *interface-type* *interface-number*
  - 3. Enable unified secure MAC address control for port security access users.  
**port-security user-mac control enable**
- By default, unified secure MAC address control for access users is not enabled.

## Command reference

### New command: port-security user-mac control enable

Use **port-security user-mac control enable** to enable the port security unified secure MAC address control for access users.

Use **undo port-security user-mac control enable** command to disable unified secure MAC control for access users.

#### Syntax

**port-security user-mac control enable**  
**undo port-security user-mac control enable**

#### Default

Unified secure MAC control for access users is disabled.

#### Views

Layer 2 Ethernet interface view

#### Predefined user roles

network-admin

#### Usage guidelines

##### Application scenarios

By default, only the MAC addresses manually configured or automatically learned in the port security autoLearn mode are considered secure MAC addresses and are subject to related security features.

To enhance network access security, the device now supports unified secure MAC management for various access users on a port.

##### About this feature

With this feature enabled on a port, the MAC addresses of 802.1X authentication users, MAC authentication users, Web authentication users, and voice VLAN users who have successfully authenticated on the port will be added to the secure MAC table and controlled by related secure MAC functions. For example, the maximum number of secure MAC addresses on the port can be deleted using the **undo port-security mac-address security sticky** command, and support for intrusion detection on the port.

For successfully authenticated 802.1X, MAC authentication, Web authentication, and voice VLAN users, their secure MAC addresses are sticky MAC addresses. You can convert them to dynamic secure MACs by using the **port-security mac-address dynamic** command.

In contrast to sticky MAC entries generated in autoLearn mode, the sticky MAC entries for authenticated users and voice VLAN users do not age while they are online. These entries are only affected by timing and traffic aging mechanisms after the users go offline.

##### Prerequisites

Before configuring this feature, you must first set the maximum number of secure MAC addresses allowed on a port by executing the **port-security max-mac-count** command in interface view. After this feature is configured, you cannot change the limit on the number of secure MAC addresses on a port.

### Restrictions and guidelines

This feature and the autoLearn mode are mutually exclusive.

When the **dot1x port-method portbased** command or **mac-authentication host-mode multi-vlan** command is configured on a port, only the MAC address of the first authenticated user is added as a secure MAC address.

### Examples

# Enable unified secure MAC address control for access users.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] port-security max-mac-count 10
[Sysname-GigabitEthernet 1/0/1] port-security user-mac control enable
```

### Related commands

**display port-security mac-address security**

Modified command: display port-security mac-address security

### Syntax

```
display port-security mac-address security [ interface interface-type
interface-number ] [ vlan vlan-id ] [ count ]
```

### Views

Any view

### Change description

The **Type** field was added to the command output to display the type (or origin) of the secure MAC address.

Example:

# Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
MAC addr          VLAN ID  State          Port index      Type           Aging time
0002-0002-0002    1        Secure         GE1/0/1         MAC-Auth       Not aged
```

--- Number of secure MAC addresses: 1 ---

# Display the number of secure MAC addresses.

```
<Sysname> display port-security mac-address security count
```

--- Number of secure MAC addresses: 1 ---

**Table 1 Command output**

| Field    | Description                     |
|----------|---------------------------------|
| MAC addr | Secure MAC address.             |
| VLAN ID  | VLAN to which the port belongs. |
| State    | MAC address type.               |

| Field                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <ul style="list-style-type: none"> <li><b>Secure</b>—Indicates that this entry is a secure MAC address entry.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                              |
| Port index                     | Port where the security MAC address entry resides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Type                           | Type (or origin) of the secure MAC address. <ul style="list-style-type: none"> <li><b>Autolearn</b>—Automatically learned.</li> <li><b>Manual</b>—Manually configured.</li> <li><b>MAC-Auth</b>—MAC authentication user.</li> <li><b>802.1X</b>—802.1X authentication user.</li> <li><b>Web-Auth</b>—Web authentication user.</li> <li><b>Voice VLAN</b>—Voice VLAN user.</li> </ul>                                                                                                                                  |
| Aging time                     | Remaining lifetime of the secure MAC address. <ul style="list-style-type: none"> <li>For static MAC addresses, this field displays <b>Not aged</b>.</li> <li>For sticky MAC addresses, this field displays the specific remaining lifetime. If the lifetime is less than 60 seconds, it is displayed in seconds. If the lifetime is 60 seconds or longer, it is displayed in minutes. Under the default setting, aging is not performed for sticky MAC addresses, and this field displays <b>Not aged</b>.</li> </ul> |
| Number of secure MAC addresses | Current number of saved secure MAC addresses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Modified feature: Configuring the padding mode and padding format for the Circuit ID sub-option

### Feature change description

As from this release, the `dhcp relay information circuit-id` command supports the **sysname** keyword. This keyword enables the device to insert the system name into the Circuit ID suboption.

### Command changes

#### Modified command: dhcp relay information circuit-id

##### Old syntax

```
dhcp relay information circuit-id { bas | string circuit-id | { normal |
verbose [ node-identifier { mac | sysname | user-defined node-identifier } ]
[ interface ] } [ format { ascii | hex } ] }
undo dhcp relay information circuit-id
```

##### New syntax

```
dhcp relay information circuit-id { bas | string circuit-id | sysname |
{ normal | verbose [ node-identifier { mac | sysname | user-defined
node-identifier } ] [ interface ] } [ format { ascii | hex } ] }
undo dhcp relay information circuit-id
```

### Views

Interface view

## Change description

Before modification: This command does not support the **sysname** keyword.

After modification: This command supports the **sysname** keyword. This keyword enables the device to insert the system name into the Circuit ID suboption. To configure the system name of a device, use the **sysname** command in system view.

## Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option

### Feature change description

As from this release, the **dhcp relay information remote-id** command supports the **interface** and **hex remote-id** parameters. The **interface** keyword enables the device to insert the interface index of the interface that received the DHCP request into the Remote ID suboption. The **hex remote-id** option enables the device to insert the user-defined hexadecimal string into the Remote ID suboption.

### Command changes

Modified command: **dhcp relay information remote-id**

#### Old syntax

```
dhcp relay information remote-id { normal [ format { ascii | hex } ] | string
remote-id | sysname }
undo dhcp relay information remote-id
```

#### New syntax

```
dhcp relay information remote-id { interface | hex remote-id | normal
[ format { ascii | hex } ] | string remote-id | sysname }
undo dhcp relay information remote-id
```

#### Views

Interface view

## Change description

Before modification: The **interface** and **hex remote-id** parameters are not supported.

After modification: The **interface** and **hex remote-id** parameters are not supported. The **interface** keyword enables the device to insert the interface index of the interface that received the DHCP request into the Remote ID suboption. For example, if the interface that received the DHCP request is GE2/0/1, the device will insert interface index 1 into the Remote ID suboption. The **hex remote-id** option enables the device to insert the user-defined hexadecimal string into the Remote ID suboption. The user-defined hexadecimal string contains 2 to 256 characters and its length must be even.

# Release 6363

This release has the following changes:

- New feature: Enabling port selection preemption on an aggregate interface
- New feature: Configuring an interface as an uplink interface to disable it from learning ARP snooping entries
- New feature: Configuring spanning tree blackhole detection
- New feature: LLDP back hole detection
- New feature: LLDP cross-domain detection
- New feature: Using the subscriber ID as the client ID in all received DHCP requests
- New feature: Configuring resource monitoring
- New feature: Sending EAP-Success packets upon successful authorization in 802.1X
- Modified feature: Support for specifying a custom hexadecimal string as the content of the Remote ID sub-option
- Modified feature: Support for specifying a custom ASCII string as the client ID of a static binding

## New feature: Enabling port selection preemption on an aggregate interface

### Enabling port selection preemption on an aggregate interface

#### About this task

When port A fails in a dynamic aggregation group, the device selects the highest priority member port, port B for example, as the new selected port. If port selection preemption is enabled and port A recovers from failure, it replaces port B. If port selection preemption is disabled, port B is still selected even though port A has higher priority, and traffic loss caused by selected port preemption is reduced.

If port selection preemption is enabled and port A recovers from failure, it immediately replaces port B. This might cause packet loss if port A's link status is unstable. To avoid this issue, configure a port selection preemption delay.

#### Procedure

1. Enter system view.  
**system-view**
2. Enter aggregate interface view.
  - Enter Layer 2 aggregate interface view.  
**interface bridge-aggregation** *interface-number*
  - Enter Layer 3 aggregate interface view.  
**interface route-aggregation** *interface-number*
3. Enable port selection preemption on an aggregate interface.  
**lACP preempt enable**  
By default, port selection preemption is enabled on an aggregate interface.
4. Set the port selection preemption delay on an aggregate interface.  
**lACP preempt delay** *delay-time*

By default, the port selection preemption delay is 0 seconds on an aggregate interface, which means port selection preemption is performed without delay.

## Command reference

### lacp preempt delay

Use **lacp preempt delay** to set the port selection preemption delay on an aggregate interface.

Use **undo lacp preempt delay** to restore the default.

#### Syntax

**lacp preempt delay** *delay-time*

**undo lacp preempt delay**

#### Default

On an aggregate interface, the port selection preemption delay is 0 seconds, which means port selection preemption is performed without delay.

#### Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

#### Predefined user roles

network-admin

#### Parameters

*delay-time*: Sets the port selection preemption delay in seconds. The value range for this argument is 10 to 180.

#### Usage guidelines

When port A fails in a dynamic aggregation group, the device selects the highest priority member port, port B for example, as the new selected port. If port selection preemption is enabled and port A recovers from failure, it immediately replaces port B. This might cause packet loss if port A's link status is unstable. To avoid this issue, configure a port selection preemption delay.

#### Examples

# Set the port selection preemption delay to 100 seconds on an aggregate interface.

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

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] lacp preempt delay 100
```

### lacp preempt enable

Use **lacp preempt enable** to enable port selection preemption.

Use **undo lacp preempt enable** to disable port selection preemption.

#### Syntax

**lacp preempt enable**

**undo lacp preempt enable**

#### Default

Port selection preemption is enabled on an aggregate interface.



## Views

Layer 2 aggregate interface view

Layer 3 aggregate interface view

## Predefined user roles

network-admin

## Usage guidelines

When port A fails in a dynamic aggregation group, the device selects the highest priority member port, port B for example, as the new selected port. If port selection preemption is enabled and port A recovers from failure, it replaces port B. If port selection preemption is disabled, port B is still selected even though port A has higher priority, and traffic loss caused by selected port preemption is reduced.

## Examples

# Disable port selection preemption on an aggregate interface.

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

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] undo lacp preempt enable
```

# New feature: Configuring an interface as an uplink interface to disable it from learning ARP snooping entries

## Configuring an interface as an uplink interface to disable it from learning ARP snooping entries

### About this task

After you enable ARP snooping on an access device by using the **arp snooping enable** command, the access device will generate ARP snooping entries by listening to ARP packets. In a network where the aggregate device acts as the gateway, if you enable local proxy ARP on the gateway by using the **local-proxy-arp enable** command, the uplink interface of the access device will also learn ARP snooping entries. As a result, the incoming interface of an ARP snooping entry flaps between the uplink and downlink interfaces. To avoid such an issue, you can configure this feature on the access device.

After you configure this feature on an access device enabled with ARP snooping, the interface no longer learns ARP snooping entries from incoming ARP packets.

### Procedure

1. Enter system view.

```
system-view
```

2. Enter interface view.

```
interface interface-type interface-number
```

Supported interface types include Layer 2 Ethernet interface and Layer 2 aggregate interface.

3. Configure the interface as an uplink interface to disable it from learning ARP snooping entries.

```
arp snooping uplink
```

By default, an interface is not an uplink interface for ARP snooping. After you enable ARP snooping, the interface learns ARP snooping entries.

# Command reference

## arp snooping uplink

Use **arp snooping uplink** to configure an interface as an uplink interface to disable it from learning ARP snooping entries.

Use **undo arp snooping uplink** to restore the default.

### Syntax

**arp snooping uplink**

**undo arp snooping uplink**

### Default

An interface is not an uplink interface for ARP snooping. After you enable ARP snooping, the interface learns ARP snooping entries.

### Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Usage guidelines

After you enable ARP snooping on an access device by using the **arp snooping enable** command, the access device will generate ARP snooping entries by listening to ARP packets. In a network where the aggregate device acts as the gateway, if you enable local proxy ARP on the gateway by using the **local-proxy-arp enable** command, the uplink interface of the access device will also learn ARP snooping entries. As a result, the incoming interface of an ARP snooping entry flaps between the uplink and downlink interfaces. To avoid such an issue, you can configure this feature on the access device.

After you configure this feature on an access device enabled with ARP snooping, the interface no longer learns ARP snooping entries from incoming ARP packets.

### Examples

# Configure Layer 2 Ethernet interface GigabitEthernet1/0/1 as an uplink interface to disable it from learning ARP snooping entries.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] arp snooping uplink
```

# Configure Layer 2 aggregate interface Bridge-Aggregation 1 as an uplink interface to disable it from learning ARP snooping entries.

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

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] arp snooping uplink
```

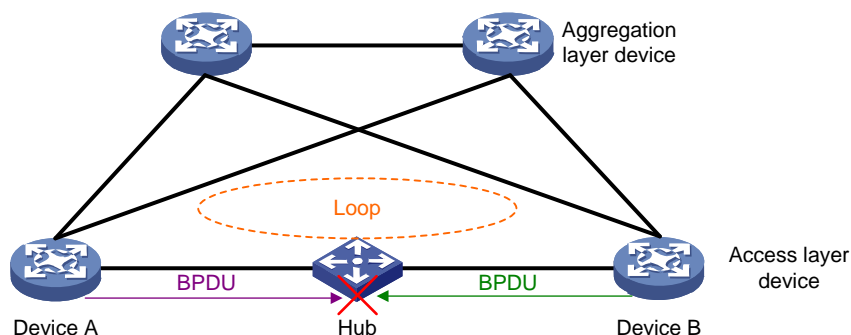
# New feature: Configuring spanning tree blackhole detection

## Configuring spanning tree blackhole detection

### About this task

As shown in the following figure, Device A and Device B are connected via a HUB, which creates a loop in the network. Since BPDUs are point-to-point frames, once they are transmitted from a device and received by the next node, their transmission is terminated. The HUB acts as a blackhole for BPDUs. BPDUs cannot be transmitted between Device A and Device B through the HUB, and Device A and Device B cannot eliminate the loop through correct spanning tree topology calculation. Therefore, a method to detect BPDU blackholes is crucial for devices to block links to blackholes when detecting them, effectively eliminating potential loop risks.

**Figure 1 Network diagram**



Spanning tree blackhole detection feature can detect the presence of BPDU blackholes in the port links. Its working mechanism is as follows.

#### 1. Blackhole verification phase.

A port enabled with spanning tree blackhole detection will start the BPDU reception timer of the blackhole detection feature. If the port receives a BPDU before the BPDU reception timer expires, the port resets the BPDU reception timer. If the BPDU reception timer expires, BPDU blackholes might exist on the network. As a result, the device fails to receive BPDUs for a long time, and the port starts to send spanning tree blackhole detection packets continuously.

Spanning tree blackhole detection packet is a type of Layer 2 packets defined by HPE. Different from the BPDU, the spanning tree blackhole detection packet can be transparently transmitted by the HUB, and will be sent continuously at a fixed time interval after being triggered to send.

Use the `stp global blackhole-detection rx-bpdu timeout` command to set the BPDU reception timer. Use the `stp timer blackhole-detection-interval` or `stp global timer blackhole-detection-interval` command to set the interval for sending spanning tree blackhole detection packets.

#### 2. Blackhole confirmation phase.

If the port is triggered to send spanning tree blackhole detection packets and receives a BPDU, it proves that no BPDU blackhole exist between the devices. The port stops transmitting the spanning tree blackhole detection packets and resets the BPDU reception timer.

If a port with the spanning tree blackhole detection feature enabled receives a blackhole detection frame while its BPDU reception timer is in a timeout state, it indicates that the link between the local and remote devices is connected. Both devices are capable of sending BPDUs, but neither device receives BPDUs. The local device determines that a BPDU blackhole exists between the two ends of the link.

#### 3. Blackhole handling phase.

After the device discovers a BPDU blackhole, it blocks the port that receives the spanning tree blackhole detection packet. Loops in the network are eliminated by preventing ports from sending and receiving any user data packets. You can use the **stp timer rx-blackhole-timeout** or **stp global timer rx-blackhole-timeout** command to specify the timeout period of the blocked port for spanning tree blackhole detection. If the port does not receive the spanning tree blackhole detection packet again within the timeout period, it means that the BPDU blackhole is eliminated, and the port returns to the normal forwarding state. Otherwise, the port continues to retain the blocking state.

The **stp timer blackhole-detection-interval** and **stp global timer blackhole-detection-interval** commands affect the frequency at which the specified port sends spanning tree blackhole detection packets. Set an appropriate packet sending interval as needed.

- When the sending interval is short, the port sends spanning tree blackhole packets more frequently. The advantage is that the network is more sensitive in detection and response to BPDU blackholes. The disadvantage is that it takes up more device CPU resources. Set a short sending interval in scenarios with strong device performance or a strong need to prevent loops.
- When the sending interval is long, the port sends spanning tree blackhole packets slowly. The advantage is that it occupies less CPU resources of the device. The disadvantage is that the network detects and responds more slowly to BPDU blackholes. Set a long sending interval in the scenario where the device performance is weak or tolerant of loops.

## Restrictions and guidelines

The spanning tree blackhole detection feature takes effect when the following conditions are met:

- On the devices at both ends of a link, the spanning tree blackhole detection is enabled both globally and on ports.
- The link status of the port on which the spanning tree blackhole detection is enabled is up, and the spanning tree feature is enabled.

If the spanning tree blackhole detection is disabled on the port, or the BPDU reception timer on the port has not expired, the port does not perform any processing after receiving the spanning tree blackhole detection packet.

On a device with a long interval for sending BPDUs, set a longer value for the BPDU reception timer to prevent the device port from being blocked when no BPDU blackhole exists on the network. On the device with a short interval for sending BPDUs, set a shorter value for the BPDU reception timer to improve the network's detection speed of BPDU blackholes.

You can use the **stp timer blackhole-detection-interval** and **stp global timer blackhole-detection-interval** commands to modify the interval for sending spanning tree blackhole detection packets on a port. When both commands are configured at the same time, the configuration of the **stp timer blackhole-detection-interval** command takes effect. If no command is configured on the port, the port inherits the configuration of the **stp global timer blackhole-detection-interval** command.

You can use the **stp timer rx-blackhole-timeout** and **stp global timer rx-blackhole-timeout** commands to modify the timeout timer for receiving spanning tree blackhole detection packets on a port. When both commands are configured at the same time, the configuration of the **stp timer rx-blackhole-timeout** command takes effect. If no command is configured on the port, the port inherits the configuration of the **stp global timer rx-blackhole-timeout** command.

## Procedure

1. Enter system view.  
**system-view**
2. Enable spanning tree blackhole detection globally.  
**stp global blackhole-detection enable**

By default, spanning tree blackhole detection is disabled globally.

3. (Optional.) Set the BPDU reception timer for the blackhole detection feature.

```
stp global blackhole-detection rx-bpdu timeout timeout
```

By default, the BPDU reception timer of the blackhole detection feature is 18 seconds.

4. (Optional.) Set the interval for sending spanning tree blackhole detection packets globally.

```
stp global timer blackhole-detection-interval interval
```

By default, the interval for sending spanning tree blackhole detection packets is 2 seconds.

5. (Optional.) Set the detection packet reception timer for spanning tree blackhole detection globally.

```
stp global timer rx-blackhole-timeout timeout
```

By default, the formula for calculating the timeout period (seconds) for receiving spanning tree blackhole packets is: Multiply the sending interval of spanning tree blackhole detection packets on a port by 3 and add 10.

6. Enter Layer 2 Ethernet interface view.

```
interface interface-type interface-number
```

7. (Optional.) Enable spanning tree blackhole detection on the port.

```
stp blackhole-detection enable
```

By default, spanning tree blackhole detection on the port is enabled.

8. (Optional.) Set the interval for sending spanning tree blackhole detection packets on the port.

```
stp timer blackhole-detection-interval interval
```

By default, the interval for sending spanning tree blackhole detection packets is 2 seconds.

9. (Optional.) Set the detection packet reception timer for spanning tree blackhole detection on the port.

```
stp timer rx-blackhole-timeout timeout
```

By default, the formula for calculating the timeout period (seconds) for receiving spanning tree blackhole packets on the port is: Multiply the sending interval of spanning tree blackhole detection packets on a port by 3 and add 10.

## Command changes

### display stp blackhole-detection blocked-port

Use **display stp blackhole-detection blocked-port** to display information about ports blocked by the spanning tree blackhole detection feature.

#### Syntax

```
display stp blackhole-detection blocked-port
```

#### Views

Any view

#### Predefined user roles

network-admin

network-operator

#### Examples

# Display the information about ports blocked by the spanning tree blackhole detection feature.

```
<Sysname> display stp blackhole-detection blocked-port
```

```
Blocked Port: Bridge-Aggregation1
```

**Table 1 Command output**

| Field        | Description                                                     |
|--------------|-----------------------------------------------------------------|
| Blocked Port | Names of the port blocked by spanning tree blackhole detection. |

## stp blackhole-detection enable

Use **stp blackhole-detection enable** to enable spanning tree blackhole detection on a port.

Use **undo stp blackhole-detection enable** to disable spanning tree blackhole detection on a port.

### Syntax

**stp blackhole-detection enable**

**undo stp blackhole-detection enable**

### Default

The spanning tree blackhole detection on a port is enabled.

### Views

Layer 2 Ethernet interface view

### Predefined user roles

network-admin

### Usage guidelines

#### Prerequisite

The spanning tree blackhole detection feature takes effect when the following conditions are met:

- On the devices at both ends of a link, the spanning tree blackhole detection is enabled both globally and on ports.
- The link status of the port on which the spanning tree blackhole detection is enabled is up, and the spanning tree feature is enabled.

#### Operating mechanism

- Blackhole verification phase.

A port enabled with spanning tree blackhole detection will start the BPDU reception timer of the blackhole detection feature. If the port receives a BPDU before the BPDU reception timer expires, the port resets the BPDU reception timer. If the BPDU reception timer expires, BPDU blackholes might exist on the network. As a result, the device fails to receive BPDUs for a long time, and the port starts to send spanning tree blackhole detection packets continuously.

Spanning tree blackhole detection packet is a type of Layer 2 packets defined by HPE. Different from the BPDU, the spanning tree blackhole detection packet can be transparently transmitted by the HUB, and will be sent continuously at a fixed time interval after being triggered to send.

Use the **stp global blackhole-detection rx-bpdu timeout** command to set the BPDU reception timer. Use the **stp timer blackhole-detection-interval** or **stp global timer blackhole-detection-interval** command to set the interval for sending spanning tree blackhole detection packets.

- Blackhole confirmation phase.

If the port is triggered to send spanning tree blackhole detection packets and receives a BPDU, it proves that no BPDU blackhole exist between the devices. The port stops transmitting the spanning tree blackhole detection packets and resets the BPDU reception timer.

If a port with the spanning tree blackhole detection feature enabled receives a blackhole detection frame while its BPDU reception timer is in a timeout state, it indicates that the link between the local and remote devices is connected. Both devices are capable of sending BPDUs, but neither device receives BPDUs. The local device determines that a BPDU blackhole exists between the two ends of the link.

### 3. Blackhole handling phase.

After the device discovers a BPDU blackhole, it blocks the port that receives the spanning tree blackhole detection packet. Loops in the network are eliminated by preventing ports from sending and receiving any user data packets. You can use the **stp timer rx-blackhole-timeout** or **stp global timer rx-blackhole-timeout** command to specify the timeout period of the blocked port for spanning tree blackhole detection. If the port does not receive the spanning tree blackhole detection packet again within the timeout period, it means that the BPDU blackhole is eliminated, and the port returns to the normal forwarding state. Otherwise, the port continues to retain the blocking state.

### Restrictions and guidelines

If the spanning tree blackhole detection is disabled on the port, or the BPDU reception timer on the port has not expired, the port does not perform any processing after receiving the spanning tree blackhole detection packet.

### Examples

```
# Enable spanning tree blackhole detection on Ten-GigabitEthernet3/0/1.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] stp blackhole-detection enable
```

### Related commands

```
stp timer rx-blackhole-timeout
stp global blackhole-detection enable
stp global blackhole-detection rx-bpdu timeout
stp global timer rx-blackhole-timeout
stp global timer blackhole-detection-interval
stp timer blackhole-detection-interval
```

### stp global blackhole-detection enable

Use **stp global blackhole-detection enable** to enable spanning tree blackhole detection globally.

Use **undo stp global blackhole-detection enable** to disable spanning tree blackhole detection globally.

### Syntax

```
stp global blackhole-detection enable
undo stp global blackhole-detection enable
```

### Default

The spanning tree blackhole detection is disabled globally.

### Views

System view

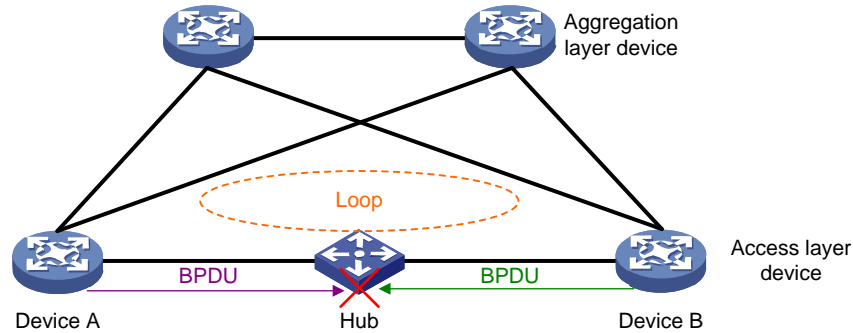
## Predefined user roles

network-admin

## Usage guidelines

### Application scenarios

Figure 2 Network diagram



As shown in Figure 2, Device A and Device B are connected via a HUB, which creates a loop in the network. Since BPDUs are point-to-point frames, once they are transmitted from a device and received by the next node, their transmission is terminated. The HUB acts as a blackhole for BPDUs. BPDUs cannot be transmitted between Device A and Device B through the HUB, and Device A and Device B cannot eliminate the loop through correct spanning tree topology calculation. Therefore, a method to detect BPDU blackholes is crucial for devices to block links to blackholes when detecting them, effectively eliminating potential loop risks.

### Prerequisite

The spanning tree blackhole detection feature takes effect when the following conditions are met:

- On the devices at both ends of a link, the spanning tree blackhole detection is enabled both globally and on ports.
- The link status of the port on which the spanning tree blackhole detection is enabled is up, and the spanning tree feature is enabled.

### Operating mechanism

#### 1. Blackhole verification phase.

A port enabled with spanning tree blackhole detection will start the BPDU reception timer of the blackhole detection feature. If the port receives a BPDU before the BPDU reception timer expires, the port resets the BPDU reception timer. If the BPDU reception timer expires, BPDU blackholes might exist on the network. As a result, the device fails to receive BPDUs for a long time, and the port starts to send spanning tree blackhole detection packets continuously.

Spanning tree blackhole detection packet is a type of Layer 2 packets defined by HPE. Different from the BPDU, the spanning tree blackhole detection packet can be transparently transmitted by the HUB, and will be sent continuously at a fixed time interval after being triggered to send.

Use the `stp global blackhole-detection rx-bpdu timeout` command to set the BPDU reception timer. Use the `stp timer blackhole-detection-interval` or `stp global timer blackhole-detection-interval` command to set the interval for sending spanning tree blackhole detection packets.

#### 2. Blackhole confirmation phase.

If the port is triggered to send spanning tree blackhole detection packets and receives a BPDU, it proves that no BPDU blackhole exist between the devices. The port stops transmitting the spanning tree blackhole detection packets and resets the BPDU reception timer.

If a port with the spanning tree blackhole detection feature enabled receives a blackhole detection frame while its BPDU reception timer is in a timeout state, it indicates that the link between the local and remote devices is connected. Both devices are capable of sending



BPDUs, but neither device receives BPDUs. The local device determines that a BPDU blackhole exists between the two ends of the link.

### 3. Blackhole handling phase.

After the device discovers a BPDU blackhole, it blocks the port that receives the spanning tree blackhole detection packet. Loops in the network are eliminated by preventing ports from sending and receiving any user data packets. You can use the **stp timer rx-blackhole-timeout** or **stp global timer rx-blackhole-timeout** command to specify the timeout period of the blocked port for spanning tree blackhole detection. If the port does not receive the spanning tree blackhole detection packet again within the timeout period, it means that the BPDU blackhole is eliminated, and the port returns to the normal forwarding state. Otherwise, the port continues to retain the blocking state.

### Restrictions and guidelines

If the spanning tree blackhole detection is disabled on the port, or the BPDU reception timer on the port has not expired, the port does not perform any processing after receiving the spanning tree blackhole detection packet.

### Examples

```
# Enable spanning tree blackhole detection globally.  
<Sysname> system-view  
[Sysname] stp global blackhole-detection enable
```

### Related commands

```
stp blackhole-detection enable  
stp timer rx-blackhole-timeout  
stp global blackhole-detection rx-bpdu timeout  
stp global timer rx-blackhole-timeout  
stp global timer blackhole-detection-interval  
stp timer blackhole-detection-interval
```

### stp global blackhole-detection rx-bpdu timeout

Use **stp global blackhole-detection rx-bpdu timeout** to set the BPDU reception timer for the blackhole detection feature.

Use **undo stp global blackhole-detection rx-bpdu timeout** to restore the default.

### Syntax

```
stp global blackhole-detection rx-bpdu timeout timeout  
undo stp global blackhole-detection rx-bpdu timeout
```

### Default

The BPDU reception timer of the blackhole detection feature is 18 seconds.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*Timeout*: Specifies the BPDU reception timer of the blackhole detection feature, in the range of 1 to 32768 seconds.

## Usage guidelines

### Operating mechanism

When the spanning tree blackhole detection is enabled both globally and on ports, a port enabled with spanning tree blackhole detection will start the BPDU reception timer of the blackhole detection feature. If the port receives a BPDU before the BPDU reception timer expires, the port resets the BPDU reception timer. If the BPDU reception timer expires, BPDU blackholes might exist on the network. As a result, the device fails to receive BPDUs for a long time, and the port starts to send spanning tree blackhole detection packets continuously.

### Restrictions and guidelines

On a device with a long interval for sending BPDUs, set a longer value for the BPDU reception timer to prevent the device port from being blocked when no BPDU blackhole exists on the network. On the device with a short interval for sending BPDUs, set a shorter value for the BPDU reception timer to improve the network's detection speed of BPDU blackholes.

Only when the link status of the port is up and the spanning tree feature is enabled, the BPDU reception timer can be enabled on the port.

## Examples

```
# Set the BPDU reception timer for the blackhole detection feature to 20 seconds.
```

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

```
[Sysname] stp global blackhole-detection rx-bpdu timeout 20s
```

## Related commands

```
stp blackhole-detection enable
```

```
stp global blackhole-detection enable
```

## stp global timer blackhole-detection-interval

Use **stp global timer blackhole-detection-interval** to set the interval for sending spanning tree blackhole detection packets globally.

Use **undo global stp timer blackhole-detection-interval** to restore the default.

## Syntax

```
stp global timer blackhole-detection-interval interval
```

```
undo stp global timer blackhole-detection-interval
```

## Default

The interval for sending spanning tree blackhole detection packets is 2 seconds

## Views

System view

## Predefined user roles

network-admin

## Parameters

*interval*: Specifies the interval for sending spanning tree blackhole detection packets, in the range of 1 to 32768 seconds

## Usage guidelines

### Recommended configuration

This command affects the frequency at which the specified port sends spanning tree blackhole detection packets. Set an appropriate packet sending interval as needed.

- When the sending interval is short, the port sends spanning tree blackhole packets more frequently. The advantage is that the network is more sensitive in detection and response to BPDU blackholes. The disadvantage is that it takes up more device CPU resources. Set a short sending interval in scenarios with strong device performance or a strong need to prevent loops.
- When the sending interval is long, the port sends spanning tree blackhole packets slowly. The advantage is that it occupies less CPU resources of the device. The disadvantage is that the network detects and responds more slowly to BPDU blackholes. Set a long sending interval in the scenario where the device performance is weak or tolerant of loops.

### Operating mechanism

You can use the **stp timer blackhole-detection-interval** and **stp global timer blackhole-detection-interval** commands to modify the interval for sending spanning tree blackhole detection packets on a port. When both commands are configured at the same time, the configuration of the **stp timer blackhole-detection-interval** command takes effect. If no command is configured on the port, the port inherits the configuration of the **stp global timer blackhole-detection-interval** command.

### Examples

```
# Set the interval for sending spanning tree blackhole detection packets to 4 seconds globally.
<Sysname> system-view
[Sysname] stp global timer blackhole-detection-interval 4
```

### Related commands

```
stp blackhole-detection enable
stp global blackhole-detection enable
stp timer blackhole-detection-interval
```

## stp global timer rx-blackhole-timeout

Use **stp global timer rx-blackhole-timeout** to set the detection packet reception timer for spanning tree blackhole detection globally.

Use **undo stp global timer rx-blackhole-timeout** to restore the default.

### Syntax

```
stp global timer rx-blackhole-timeout timeout
undo stp global timer rx-blackhole-timeout
```

### Default

The formula for calculating the timeout period (seconds) for receiving spanning tree blackhole packets is: Multiply the sending interval of spanning tree blackhole detection packets on a port by 3 and add 10.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*timeout*: Specifies the detection packet reception timer for spanning tree blackhole detection, in the range of 10 to 65535 seconds.

### Usage guidelines

#### Operating mechanism

After the port is blocked by the spanning tree blackhole detection, the timer for receiving spanning tree blackhole detection packets is started. Before the timer expires, the port will reset the timer when it receives a spanning tree blackhole detection packet, and remain in the blocking state. After the timer expires, the port returns to the normal forwarding state.

### Restrictions and guidelines

You can use the `stp timer rx-blackhole-timeout` and `stp global timer rx-blackhole-timeout` commands to modify the interval for sending spanning tree blackhole detection packets on a port. When both commands are configured at the same time, the configuration of the `stp timer rx-blackhole-timeout` command takes effect. If no command is configured on the port, the port inherits the configuration of the `stp global timer rx-blackhole-timeout` command.

### Examples

```
# Set the detection packet reception timer for spanning tree blackhole detection to 12 seconds globally.
```

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

```
[Sysname] stp global timer rx-blackhole-timeout 12
```

### Related commands

```
stp blackhole-detection enable
```

```
stp global blackhole-detection enable
```

```
stp timer rx-blackhole-detection
```

### stp timer blackhole-detection-interval

Use `stp timer blackhole-detection-interval` to set the interval for sending spanning tree blackhole detection packets on a port.

Use `undo stp timer blackhole-detection-interval` to restore the default.

### Syntax

```
stp timer blackhole-detection-interval interval
```

```
undo stp timer blackhole-detection-interval
```

### Default

The interval for sending spanning tree blackhole detection packets on a port is 2 seconds.

### Views

Layer 2 Ethernet interface view

### Predefined user roles

network-admin

### Parameters

*interval*: Specifies the interval for sending spanning tree blackhole detection packets, in the range of 10 to 32768 seconds.

### Usage guidelines

#### Recommended configuration

This command affects the frequency at which the specified port sends spanning tree blackhole detection packets. Set an appropriate packet sending interval as needed.

- When the sending interval is short, the port sends spanning tree blackhole packets more frequently. The advantage is that the network is more sensitive in detection and response to

BPDUs blackholes. The disadvantage is that it takes up more device CPU resources. Set a short sending interval in scenarios with strong device performance or a strong need to prevent loops.

- When the sending interval is long, the port sends spanning tree blackhole packets slowly. The advantage is that it occupies less CPU resources of the device. The disadvantage is that the network detects and responds more slowly to BPDUs blackholes. Set a long sending interval in the scenario where the device performance is weak or tolerant of loops.

### Operating mechanism

You can use the **stp timer blackhole-detection-interval** and **stp global timer blackhole-detection-interval** commands to modify the interval for sending spanning tree blackhole detection packets on a port. When both commands are configured at the same time, the configuration of the **stp timer blackhole-detection-interval** command takes effect. If no command is configured on the port, the port inherits the configuration of the **stp global timer blackhole-detection-interval** command.

### Examples

```
# Set the interval for sending spanning tree blackhole detection packets to 4 seconds on Ten-GigabitEthernet 3/0/1.
```

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

```
[Sysname] interface ten-gigabitethernet 3/0/1
```

```
[Sysname-Ten-GigabitEthernet3/0/1] stp timer blackhole-detection-interval 4
```

### Related commands

```
stp blackhole-detection enable
```

```
stp global blackhole-detection enable
```

```
stp global timer blackhole-detection-interval
```

### stp timer rx-blackhole-timeout

Use **stp timer rx-blackhole-timeout** to set the detection packet reception timer for spanning tree blackhole detection on a port.

Use **undo stp timer rx-blackhole-timeout** to restore the default.

### Syntax

```
stp timer rx-blackhole-timeout timeout
```

```
undo timer stp rx-blackhole-timeout
```

### Default

The formula for calculating the timeout period (seconds) for receiving spanning tree blackhole packets on the port is: Multiply the sending interval of spanning tree blackhole detection packets on a port by 3 and add 10.

### Views

Layer 2 Ethernet interface view

### Predefined user roles

network-admin

### Parameters

*timeout*: Specifies the detection packet reception timer for spanning tree blackhole detection, in the range of 10 to 65535 seconds.

### Usage guidelines

#### Operating mechanism

After the port is blocked by the spanning tree blackhole detection, the timer for receiving spanning tree blackhole detection packets is started. Before the timer expires, the port will reset the timer when it receives a spanning tree blackhole detection packet, and remain in the blocking state. After the timer expires, the port returns to the normal forwarding state.

### Restrictions and guidelines

You can use the `stp timer rx-blackhole-timeout` and `stp global timer rx-blackhole-timeout` commands to modify the interval for sending spanning tree blackhole detection packets on a port. When both commands are configured at the same time, the configuration of the `stp timer rx-blackhole-timeout` command takes effect. If no command is configured on the port, the port inherits the configuration of the `stp global timer rx-blackhole-timeout` command.

### Examples

```
# Set the detection packet reception timer for spanning tree blackhole detection to 12 seconds on Ten-GigabitEthernet 3/0/1.
```

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

```
[Sysname] interface ten-gigabitethernet 3/0/1
```

```
[Sysname-Ten-GigabitEthernet3/0/1] stp timer rx-blackhole-timeout 12
```

### Related commands

```
stp blackhole-detection enable
```

```
stp global blackhole-detection enable
```

```
stp global timer rx-blackhole-detection
```

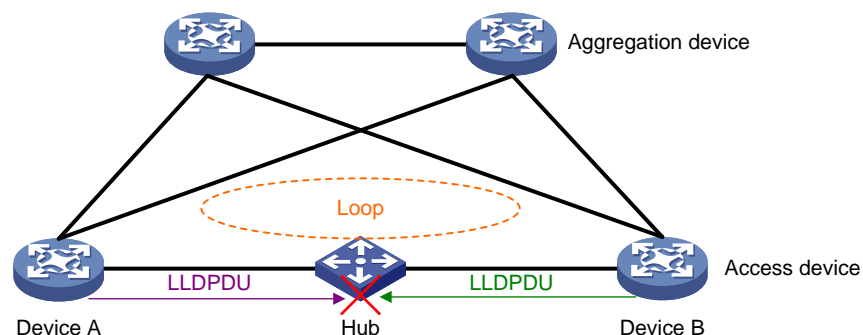
## New feature: LLDP black hole detection

### Configuring LLDP black hole detection

#### About this task

As shown in [Table 1](#) [Figure 1](#), Device A and Device B are connected through a hub, causing a loop in the network. However, since LLDP packets are point-to-point packets, they are terminated at the next node after being sent from the device. Therefore, the hub acts as a black hole for LLDP packets and LLDP packets cannot be transmitted between Device A and Device B through the HUB. As a result, Device A and Device B cannot use LLDP to learn about the physical link between them and the formed loop, and therefore the loop cannot be eliminated in time. In order to eliminate potential loop risks, it required to detect LLDP packet black holes and block the links leading to the black holes.

**Figure 2 LLDP black hole detection application scenario**



The LLDP black hole detection feature can detect the presence of LLDP black holes in links on ports. The operating mechanism is as follows:

1. Triggering the sending of black hole detection packets

The ports enabled with LLDP black hole detection will carry black hole detection TLVs in the transmitted LLDP packets. The black hole detection TLV is a type of TLV defined by HPE. If an LLDP packet carrying the black hole detection TLV is received, it indicates that there is no LLDP black hole between the device and its neighbor, and LLDP packets can be sent and received successfully. Only HPE devices can send and recognize the black hole detection TLV carried in LLDP packets.

After LLDP black hole detection is enabled on a port, the port will activate the LLDP packet receiving timer for black hole detection. If no LLDP packets are received on the port until the timer expires, it indicates a potential LLDP packet black hole in the network, causing the device to not receive LLDP packets. The port then starts sending LLDP black hole detection packets continuously. If the port receives an LLDP packet carrying the black hole detection TLV before the timer expires, the port terminates the timer and takes no further action.

After LLDP black hole detection is enabled, if a port receives an LLDP packet without the black hole detection TLV, the port will start sending LLDP black hole detection packets continuously.

LLDP black hole detection packet is an HPE proprietary Layer 2 packet type. Unlike LLDP packets, LLDP black hole detection packets can be transparently transmitted by a hub and are continuously sent at fixed intervals after being triggered.

The timeout for receiving LLDP packets is configured through the `lldp global blackhole-detection rx-lldpdu timeout` command. The interval for sending LLDP black hole detection packets is configured through the `lldp timer blackhole-detection-interval` command or the `lldp global timer blackhole-detection-interval` command.

2. Black hole confirmation

After a port starts to send LLDP black hole detection packets, if it receives an LLDP packet carrying the black hole detection TLV, it determines that no LLDP black hole exists between the port and its neighbor, stops sending LLDP black hole detection packets, and resets the LLDP packet receiving timer.

If a port enabled with LLDP black hole detection receives an LLDP black hole detection packet and the LLDP packet receiving timer on this port has timed out, it indicates that the local device and the peer device are connected with a link and both devices have the ability to send LLDP packets. However, neither of the devices has received LLDP packets, and therefore the local device concludes that there is an LLDP black hole between the two ends of the link.

3. Black hole processing

After detecting an LLDP black hole, the device blocks the port receiving LLDP black hole detection packets to eliminate network loops and prevent the transmission of user data packets. If the blocked port receives no LLDP black hole detection packets within the timeout period specified by the `lldp timer rx-blackhole-timeout` or `lldp global timer rx-blackhole-timeout` command, it means that the LLDP black hole is eliminated and the port resumes normal forwarding. Otherwise, it remains blocked.

The `lldp timer blackhole-detection-interval` and `lldp global timer blackhole-detection-interval` commands affect the interval at which the specified ports send LLDP black hole detection packets. Set a suitable packet sending interval based on actual requirements.

- When the sending interval is short, the port sends LLDP black hole detection packets frequently. The advantage is that the network detects and responds to LLDP black holes more sensitively. The disadvantage is that it occupies more device CPU resources. Configure a short sending interval in scenarios where the device performance is high or there is a strong demand for loop prevention.
- When the sending interval is long, the port sends LLDP black hole detection packets slowly. The advantage is that it occupies less CPU resources of the device; while the disadvantage is

that the device cannot detect and respond to LLDP black holes quickly. Configure longer sending intervals in scenarios where device performance is weaker or loop tolerance is higher.

## Restrictions and guidelines

The LLDP black hole detection feature takes effect only if the following conditions are met:

- On both ends of the LLDP connection, both global and port-level LLDP black hole detection functions are enabled.
- On the ports with LLDP black hole detection enabled, the link status is UP, LLDP is enabled, and the operating mode is TxRx.

If LLDP black hole detection is not enabled on a port or the LLDP packet receiving timer of the port has not timed out, the port will not process any LLDP black hole detection packets received.

On devices with a long LLDP packet sending interval, configure a longer LLDP packet receiving timeout. Otherwise, it might result in device ports being blocked even if no LLDP black hole exists in the network. Configure a shorter LLDP receiving timeout on devices with a shorter LLDP packet sending interval for more efficient LLDP black hole detection.

The `lldp timer blackhole-detection-interval` and `lldp global timer blackhole-detection-interval` commands can both set the interval at which ports send LLDP black hole detection packets. When both commands are configured, the `lldp timer blackhole-detection-interval` command takes precedence. If the interval is not set on a port, the port uses the global interval set by the `lldp global timer blackhole-detection-interval` command.

The timeout for receiving LLDP black hole detection packets on a port can be configured by using the `lldp timer rx-blackhole-timeout` and `lldp global timer rx-blackhole-timeout` commands. When both commands are configured, the `lldp timer rx-blackhole-timeout` command takes precedence. If a port is not configured with a timeout, it uses the global timeout set by the `lldp global timer rx-blackhole-timeout` command.

The timeout for receiving LLDP black hole detection packets on the local device should not be less than the interval for sending LLDP black hole detection packets on the peer device. Otherwise, LLDP black hole detection will not take effect.

## Procedure

1. Enter system view.  
**system-view**
2. Enable global LLDP black hole detection.  
**lldp global blackhole-detection enable**  
By default, global LLDP black hole detection is disabled.
3. (Optional.) Configure the LLDP packet receiving timeout for black hole detection.  
**lldp global blackhole-detection rx-lldpdu timeout**  
By default, the LLDP packet receiving timeout for black hole detection is 120 seconds.
4. (Optional.) Set the global interval for sending LLDP black hole detection packets.  
**lldp global timer blackhole-detection-interval interval**  
By default, the interval for sending LLDP black hole detection packets is 2 seconds.
5. (Optional.) Set the global timeout for receiving LLDP black hole detection packets.  
**lldp global timer rx-blackhole-timeout timeout**  
By default, the timeout for receiving LLDP black hole detection packets is (the global interval for sending LLDP black hole detection packets × 3 + 10) seconds.
6. (Optional.) Enter Layer 2 Ethernet interface view.  
**interface interface-type interface-number**



7. (Optional.) Enable LLDP black hole detection for a port.  
**lldp blackhole-detection enable**  
By default, LLDP black hole detection is enabled for a port.
8. (Optional.) Set the interval at which the port sends LLDP black hole detection packets.  
**lldp timer blackhole-detection-interval *interval***  
By default, the interval for sending LLDP black hole detection packets is 2 seconds.
9. (Optional.) Set the timeout for receiving LLDP black hole detection packets on the port.  
**lldp timer rx-blackhole-timeout *timeout***  
By default, the timeout for receiving LLDP black hole detection packets on a port is (the port's sending interval for LLDP black hole detection packets × 3 + 10) seconds.

## Command reference

### lldp blackhole-detection enable

Use **lldp blackhole-detection enable** to enable LLDP black hole detection for a port.

Use **undo lldp blackhole-detection enable** to disable LLDP black hole detection for a port.

#### Syntax

```
lldp blackhole-detection enable
undo lldp blackhole-detection enable
```

#### Default

LLDP black hole detection is enabled for a port.

#### Views

Layer 2 Ethernet interface view

#### Predefined user roles

network-admin

#### Usage guidelines

##### Prerequisites

The LLDP black hole detection feature takes effect only if the following conditions are met:

- On both ends of the LLDP connection, both global and port-level LLDP black hole detection functions are enabled.
- On the ports with LLDP black hole detection enabled, the link status is UP, LLDP is enabled, and the operating mode is TxRx.

##### Operating mechanism

1. Triggering the sending of black hole detection packets

The ports enabled with LLDP black hole detection will carry black hole detection TLVs in the transmitted LLDP packets. The black hole detection TLV is a type of TLV defined by HPE. If an LLDP packet carrying the black hole detection TLV is received, it indicates that there is no LLDP black hole between the device and its neighbor, and LLDP packets can be sent and received smoothly. Only HPE devices can send and recognize the black hole detection TLV carried in LLDP packets.

After LLDP black hole detection is enabled on a port, the port will activate the LLDP packet receiving timer for black hole detection. If no LLDP packets are received on the port until the timer expires, it indicates a potential LLDP packet black hole in the network, causing the device

to not receive LLDP packets. The port then starts sending continuous LLDP black hole detection packets. If the port receives an LLDP packet carrying the black hole detection TLV before the timer expires, the port terminates the timer and takes no further action.

After LLDP black hole detection is enabled, if a port receives an LLDP packet without the black hole detection TLV, the port will start sending LLDP black hole detection packets continuously.

LLDP black hole detection packet is an HPE proprietary Layer 2 packet type. Unlike LLDP packets, LLDP black hole detection packets can be transparently transmitted by a hub and are continuously sent at fixed intervals after being triggered.

The timeout period for receiving LLDP packets is configured by using the **lldp global blackhole-detection rx-lldpdu timeout** command. The interval for sending LLDP black hole detection packets is configured through the **lldp timer blackhole-detection-interval** command or the **lldp global timer blackhole-detection-interval** command.

## 2. Black hole confirmation

After a port starts to send LLDP black hole detection packets, if it receives an LLDP packet carrying the black hole detection TLV, it determines that no LLDP black hole exists between the port and its neighbor, stops sending LLDP black hole detection packets, and resets the LLDP packet receiving timer.

If a port enabled with LLDP black hole detection receives an LLDP black hole detection packet and the LLDP packet receiving timer on this port has timed out, it indicates that the local device and the peer device are connected with a link and both devices have the ability to send LLDP packets. However, neither of the devices has received LLDP packets, and therefore the local device concludes that there is an LLDP black hole between the two ends of the link.

## 3. Black hole processing

After detecting an LLDP black hole, the device blocks the ports receiving LLDP black hole detection packets to eliminate network loops and prevent the transmission of user data packets. If the blocked port receives no LLDP black hole detection packets within the timeout period specified by the **lldp timer rx-blackhole-timeout** or **lldp global timer rx-blackhole-timeout** command, it means that the LLDP black hole is eliminated and the port resumes normal forwarding. Otherwise, it remains blocked.

## Restrictions and guidelines

If LLDP black hole detection is not enabled on a port or the LLDP packet receiving timer of the port has not timed out, the port will not process any LLDP black hole detection packets received.

For LLDP black hole detection to take effect on a port, you must enable LLDP black hole detection globally and for that port.

## Examples

```
# Enable LLDP black hole detection on port Ten-GigabitEthernet3/0/1.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] lldp blackhole-detection enable
```

## Related commands

```
lldp blackhole-detection enable
lldp global timer rx-blackhole-timeout
lldp global blackhole-detection rx-lldpdu timeout
lldp global timer blackhole-detection-interval
lldp timer blackhole-detection-interval
lldp timer rx-blackhole-timeout
```

## lldp global blackhole-detection enable

Use `lldp global blackhole-detection enable` to enable global LLDP black hole detection.

Use `undo lldp global blackhole-detection enable` to disable global LLDP black hole detection.

### Syntax

```
lldp global blackhole-detection enable
```

```
undo lldp global blackhole-detection enable
```

### Default

Global LLDP black hole detection is disabled.

### Views

System view

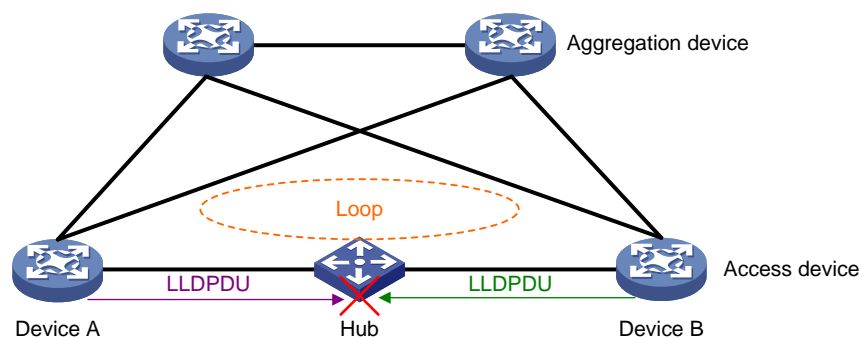
### Predefined user roles

network-admin

### Usage guidelines

#### Application scenarios

**Figure 2 LLDP black hole detection application scenario**



As shown in [Figure 2](#), Device A and Device B are connected through a hub, causing a loop in the network. However, since LLDP packets are point-to-point packets, they are terminated at the next node after being sent from the device. Therefore, the HUB acts as a black hole for LLDP packets. LLDP packets cannot be transmitted between Device A and Device B through the HUB. As a result, Device A and Device B cannot use LLDP to learn about the physical link between them and the formed loop, and therefore the loop cannot be eliminated in time. In order to eliminate potential loop risks, it required to detect LLDP black holes and block the links leading to the black holes.

### Prerequisites

The LLDP black hole detection feature takes effect only if the following conditions are met:

- On both ends of the LLDP connection, both global and port-level LLDP black hole detection functions are enabled.
- On the ports with LLDP black hole detection enabled, the link status is UP, LLDP is enabled, and the operating mode is TxRx.

### Operating mechanism

#### 1. Black hole detection

The ports enabled with LLDP black hole detection will carry black hole detection TLVs in the transmitted LLDP packets. The black hole detection TLV is a type of TLV defined by HPE. If an

LLDP packet carrying the black hole detection TLV is received, it indicates that there is no LLDP black hole between the device and its neighbor, and LLDP packets can be sent and received smoothly. Only HPE devices can send and recognize the black hole detection TLV carried in LLDP packets.

After LLDP black hole detection is enabled on a port, the port will activate the LLDP packet receiving timer for black hole detection. If no LLDP packets are received on the port until the timer expires, it indicates a potential LLDP packet black hole in the network, causing the device to not receive LLDP packets. The port then starts sending continuous LLDP black hole detection packets. If the port receives an LLDP packet carrying the black hole detection TLV before the timer expires, the port terminates the timer and takes no further action.

After LLDP black hole detection is enabled, if a port receives an LLDP packet without the black hole detection TLV, the port will start sending LLDP black hole detection packets continuously.

LLDP black hole detection packet is an HPE proprietary Layer 2 packet type. Unlike LLDP packets, LLDP black hole detection packets can be transparently transmitted by a hub and are continuously sent at fixed intervals after being triggered.

The timeout period for receiving LLDP packets is configured by using the **lldp global blackhole-detection rx-lldpdu timeout** command. The interval for sending LLDP black hole detection packets is configured through the **lldp timer blackhole-detection-interval** command or the **lldp global timer blackhole-detection-interval** command.

## 2. Black hole confirmation

After a port starts to send LLDP black hole detection packets, if it receives an LLDP packet carrying the black hole detection TLV, it determines that no LLDP black hole exists between the port and its neighbor, stops sending LLDP black hole detection packets, and resets the LLDP packet receiving timer.

If a port enabled with LLDP black hole detection receives an LLDP black hole detection packet and the LLDP packet receiving timer on this port has timed out, it indicates that the local device and the peer device are connected with a link and both devices have the ability to send LLDP packets. However, neither of the devices has received LLDP packets, and therefore the local device concludes that there is an LLDP black hole between the two ends of the link.

## 3. Black hole processing

After detecting an LLDP black hole, the device blocks the ports receiving LLDP black hole detection packets to eliminate network loops and prevent the transmission of user data packets. If the blocked port receives no LLDP black hole detection packets within the timeout period specified by the **lldp timer rx-blackhole-timeout** or **lldp global timer rx-blackhole-timeout** command, it means that the LLDP black hole is eliminated and the port resumes normal forwarding. Otherwise, it remains blocked.

## Restrictions and guidelines

If LLDP black hole detection is not enabled on a port or the LLDP packet receiving timer of the port has not timed out, the port will not process any LLDP black hole detection packets received.

## Examples

```
# Enable global LLDP black hole detection.
<Sysname> system-view
[Sysname] lldp global blackhole-detection enable
```

## Related commands

```
lldp blackhole-detection enable
lldp global timer rx-blackhole-timeout
lldp global blackhole-detection rx-lldpdu timeout
lldp global timer blackhole-detection-interval
```

```
lldp timer blackhole-detection-interval
```

```
lldp timer rx-blackhole-timeout
```

## lldp global blackhole-detection rx-lldpdu timeout

Use `lldp global blackhole-detection rx-lldpdu timeout` to configure the LLDP packet receiving timeout for black hole detection.

Use `undo lldp global blackhole-detection rx-lldpdu timeout` to restore the default.

### Syntax

```
lldp global blackhole-detection rx-lldpdu timeout
```

```
undo lldp global blackhole-detection rx-lldpdu timeout
```

### Default

The LLDP packet receiving timeout for black hole detection is 120 seconds.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*timeout*: LLDP packet receiving timeout for black hole detection, in the range of 1 to 32768, in seconds.

### Usage guidelines

#### Operating mechanism

After LLDP black hole detection is enabled on a port, the port will activate the LLDP packet receiving timer for black hole detection. If no LLDP packets are received on the port until the timer expires, it indicates a potential LLDP packet black hole in the network, causing the device to not receive LLDP packets. The port then starts sending continuous LLDP black hole detection packets. If the port receives an LLDP packet carrying the black hole detection TLV before the timer expires, the port terminates the timer and takes no further action.

#### Restrictions and guidelines

On devices with a long LLDP packet sending interval, configure a longer LLDP packet receiving timeout. Otherwise, it might result in device ports being blocked even if no LLDP black hole exists in the network. Configure a shorter LLDP receiving timeout on devices with a shorter LLDP packet sending interval for more efficient LLDP black hole detection.

The LLDP packet receiving timeout can take effect on a port only when the link state of the port is UP, LLDP is enabled on the port, and the port operates in TxRx mode.

### Examples

# Configure the LLDP packet receiving timeout for black hole detection as 140 seconds.

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

```
[Sysname] lldp global blackhole-detection rx-lldpdu timeout 140
```

### Related commands

```
lldp admin-status
```

```
lldp blackhole-detection enable
```

```
lldp global blackhole-detection enable
```

## lldp global timer blackhole-detection-interval

Use **lldp global timer blackhole-detection-interval** to configure the global interval for sending LLDP black hole detection packets.

Use **undo lldp global timer blackhole-detection-interval** to restore the default.

### Syntax

```
lldp global timer blackhole-detection-interval interval
```

```
undo lldp global timer blackhole-detection-interval
```

### Default

The interval for sending LLDP black hole detection packets is 2 seconds.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*interval*: Interval for sending LLDP black hole detection packets, in the range of 1 to 32768, in seconds.

### Usage guidelines

#### Recommended configuration

This command takes effect on all ports that have enabled LLDP black hole detection. It controls the speed at which the ports send LLDP black hole detection packets globally. Set an appropriate packet sending interval based on the actual requirements.

- When the sending interval is short, the port sends LLDP black hole detection packets frequently. The advantage is that the network detects and responds to LLDP black holes more sensitively. The disadvantage is that it occupies more device CPU resources. Configure a short sending interval in scenarios where the device performance is high or there is a strong demand for loop prevention.
- When the sending interval is long, the port sends LLDP black hole detection packets slowly. The advantage is that it occupies less CPU resources of the device; while the disadvantage is that the device cannot detect and respond to LLDP black holes quickly. Configure longer sending intervals in scenarios where device performance is weaker or loop tolerance is higher.

#### Operating mechanism

The **lldp timer blackhole-detection-interval** and **lldp global timer blackhole-detection-interval** commands can both set the interval at which ports send LLDP black hole detection packets. When both commands are configured, the **lldp timer blackhole-detection-interval** command takes precedence. If the interval is not set on a port, the port uses the global interval set by the **lldp global timer blackhole-detection-interval** command.

### Examples

```
# Set the global interval for sending LLDP black hole detection packets to 4 seconds.
```

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

```
[Sysname] lldp global timer blackhole-detection-interval 4
```

### Related commands

```
lldp blackhole-detection enable
```

```
lldp global blackhole-detection enable
lldp timer blackhole-detection-interval
```

## lldp global timer rx-blackhole-timeout

Use `lldp global timer rx-blackhole-timeout` to configure the global timeout for receiving LLDP black hole detection packets.

Use `undo lldp global timer rx-blackhole-timeout` to restore the default.

### Syntax

```
lldp global timer rx-blackhole-timeout timeout
undo lldp global timer rx-blackhole-timeout
```

### Default

The timeout for receiving LLDP black hole detection packets is (the global interval for sending LLDP black hole detection packets × 3 + 10) seconds.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*timeout*: Timeout for receiving LLDP black hole detection packets, in the range of 10 to 65535, in seconds.

### Usage guidelines

#### Operating mechanism

When a port is blocked by LLDP black hole detection, the port starts the LLDP black hole detection packet receiving timer. Before the timer times out, the port resets the timer and remains in a blocked state when it receives an LLDP black hole detection packet. After the timer times out, the port resumes normal forwarding.

#### Restrictions and guidelines

The timeout for receiving LLDP black hole detection packets on a port can be configured by using the `lldp timer rx-blackhole-timeout` and `lldp global timer rx-blackhole-timeout` commands. When both commands are configured, the `lldp timer rx-blackhole-timeout` command takes precedence. If a port is not configured with a timeout, it uses the global timeout configured by the `lldp global timer rx-blackhole-timeout` command.

The timeout for receiving LLDP black hole detection packets on the local device should not be less than the interval for sending LLDP black hole detection packets on the peer device. Otherwise, LLDP black hole detection will not take effect.

### Examples

```
# Set the global timeout for receiving LLDP black hole detection packets to 14 seconds.
<Sysname> system-view
[Sysname] lldp global timer rx-blackhole-timeout 14
```

### Related commands

```
lldp blackhole-detection enable
lldp global blackhole-detection enable
```

```
lldp global timer blackhole-detection-interval
lldp timer rx-blackhole-timeout
lldp timer blackhole-detection-interval
```

## lldp timer blackhole-detection-interval

Use `lldp timer blackhole-detection-interval` to configure the interval at which a port sends LLDP black hole detection packets.

Use `undo lldp timer blackhole-detection-interval` to restore the default.

### Syntax

```
lldp timer blackhole-detection-interval interval
undo lldp timer blackhole-detection-interval
```

### Default

A port sends LLDP black hole detection packets at intervals of 2 seconds.

### Views

Layer 2 Ethernet interface view

### Predefined user roles

network-admin

### Parameters

*interval*: Interval for sending LLDP black hole detection packets, in the range of 1 to 32768, in seconds.

### Usage guidelines

#### Recommended configuration

This command takes effect on the port where the command is executed. Set a suitable packet sending interval according to actual requirements.

- When the sending interval is short, the port sends LLDP black hole detection packets frequently. The advantage is that the network detects and responds to LLDP black holes more sensitively. The disadvantage is that it occupies more device CPU resources. Configure a short sending interval in scenarios where the device performance is high or there is a strong demand for loop prevention.
- When the sending interval is long, the port sends LLDP black hole detection packets slowly. The advantage is that it occupies less CPU resources of the device; while the disadvantage is that the device cannot detect and respond to LLDP black holes quickly. Configure longer sending intervals in scenarios where device performance is weaker or loop tolerance is higher.

#### Operating mechanism

The `lldp timer blackhole-detection-interval` and `lldp global timer blackhole-detection-interval` commands can both set the interval at which ports send LLDP black hole detection packets. When both commands are configured, the `lldp timer blackhole-detection-interval` command takes precedence. If the interval is not set on a port, the port uses the global interval set by the `lldp global timer blackhole-detection-interval` command.

### Examples

# Configure port Ten-GigabitEthernet3/0/1 to send LLDP black hole detection packets at intervals of 4 seconds.

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



```
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] lldp timer blackhole-detection-interval 4
```

## Related commands

```
lldp blackhole-detection enable
lldp global blackhole-detection enable
lldp global timer blackhole-detection-interval
```

## lldp timer rx-blackhole-timeout

Use **lldp timer rx-blackhole-timeout** to configure the timeout for receiving LLDP black hole detection packets on a port.

Use **undo lldp timer rx-blackhole-timeout** to restore the default.

## Syntax

```
lldp timer rx-blackhole-timeout timeout
undo timer lldp rx-blackhole-timeout
```

## Default

The timeout for a port to receive LLDP black hole detection packets is (the port's sending interval for LLDP black hole detection packets × 3 + 10) seconds.

## Views

Layer 2 Ethernet interface view

## Predefined user roles

network-admin

## Parameters

*timeout*: Timeout for receiving LLDP black hole detection packets, in the range of 10 to 65535, in seconds.

## Usage guidelines

### Operating mechanism

When a port is blocked by LLDP black hole detection, the port starts the LLDP black hole detection packet receiving timer. Before the timer times out, the port resets the timer and remains in a blocked state when it receives an LLDP black hole detection packet. After the timer times out, the port resumes normal forwarding.

### Restrictions and guidelines

The timeout for receiving LLDP black hole detection packets on a port can be configured by using the **lldp timer rx-blackhole-timeout** and **lldp global timer rx-blackhole-timeout** commands. When both commands are configured, the **lldp timer rx-blackhole-timeout** command takes precedence. If a port is not configured with a timeout, it uses the global timeout configured by the **lldp global timer rx-blackhole-timeout** command.

The timeout for receiving LLDP black hole detection packets on the local device should not be less than the interval for sending LLDP black hole detection packets on the peer device. Otherwise, LLDP black hole detection will not take effect.

## Examples

```
# Configure the timeout for receiving LLDP black hole detection packets as 12 seconds on port
Ten-GigabitEthernet3/0/1.
```

```

<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] lldp timer rx-blackhole-timeout 12

```

## Related commands

```

lldp blackhole-detection enable
lldp global blackhole-detection enable
lldp global timer rx-blackhole-timeout
lldp global timer blackhole-detection-interval
lldp timer blackhole-detection-interval

```

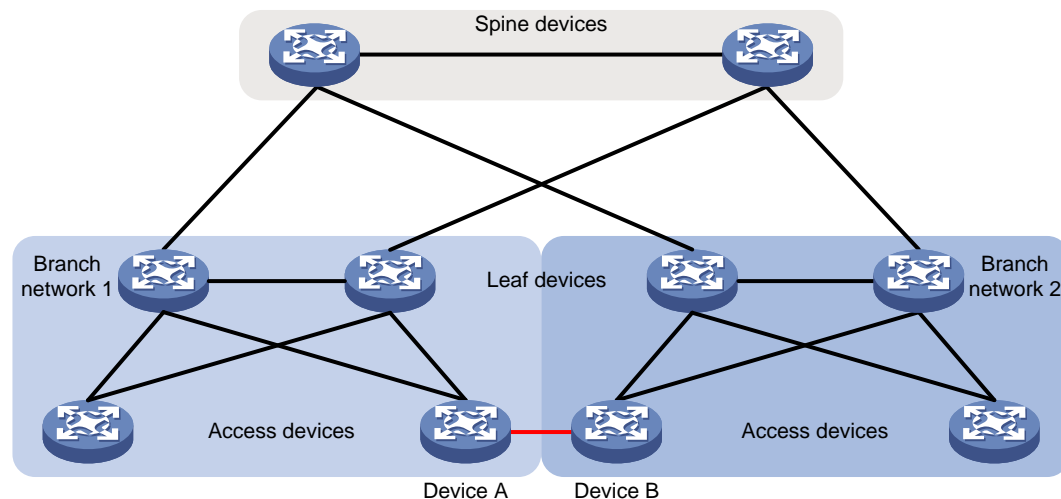
# New feature: LLDP cross-domain detection

## Configuring LLDP cross-domain detection

### About this task

As shown in [Figure 2](#), Device A and Device B belongs to different branch networks. If a link exists between Device A and Device B, a loop might occur in the network. After configuring LLDP cross-domain detection, you can manually assign the devices to different domains, and use LLDP to detect whether the specified LLDP neighbor is in the local domain. In addition, you can block the link to neighbors in other domains to eliminate the potential loop risk.

**Figure 3 LLDP cross-domain detection application scenario**



The LLDP cross-domain detection feature defines a private type of TLVs for LLDP, that is, the cross-domain detection TLVs. This TLV is used to advertise the local domain to the LLDP neighbor at the peer end. The LLDP cross-domain detection feature takes effect on a port only after you perform the following operations:

- Execute the **lldp global cross-domain-detection enable** or **lldp cross-domain-detection** command to enable LLDP cross-domain detection.
- Execute the **lldp cross-domain-detection domain-id** command to configure the domain ID for the local device.

Then, LLDP packets sent by the device will carry cross-domain detection TLVs.

A cross-domain detection TLV contains the domain ID, device bridge ID, port cost, and port ID. The device bridge ID is the bridge ID of the device that sends the cross-domain detection TLV. The port cost is the cost of the port that sends the cross-domain detection TLV. The port ID is the ID of the port that sends the cross-domain detection TLV.

Upon receiving LLDP packets carrying cross-domain detection TLVs, if the receiving ports are enabled with cross-domain detection, the device compares the domain IDs in the packets with the local setting:

- If the domain IDs are the same, the devices at the two ends of the LLDP session belong to the same domain, and the local device does not process the packets.
- If the domain IDs are different, the devices at the two ends of the LLDP session do not belong to the same domain. Data traffic transmission between each other might result in loops. To prevent this issue, the device performs the following operations:
  - If only one port receives an LLDP packet carrying the cross-domain detection TLV, the device blocks the port. In addition, it disables the port from receiving or sending any user data packets to eliminate loops in the network.
  - If multiple ports receive LLDP packets carrying the cross-domain detection TLVs with the same domain ID, the device compares the cross-domain detection TLVs received by the ports:
    - The cross-domain detection TLV received by the port with the smallest cost is the optimal TLV.
    - If the ports have the same cost, the cross-domain detection TLV received by the device with the smallest bridge ID is the optimal TLV.
    - If the devices have the same bridge ID, the cross-domain detection TLV received by the port with the smallest ID is the optimal TLV.

Except the port that receives the optimal cross-domain detection TLV, the device blocks all other ports that receive cross-domain detection TLVs. In addition, it disables the ports from receiving or sending any user data packets to eliminate loops in the network.

A blocked port can restore normal forwarding status when LLDP cross-domain detection is disabled or it receives a cross-domain detection TLV carrying the same domain ID as the local setting.

## Restrictions and guidelines

If the domain ID is not configured for LLDP cross-domain detection, or the port is not enabled with the cross-domain detection TLV advertisement capability, the cross-domain detection feature cannot take effect on the port. In this case, the device cannot identify cross-domain detection TLVs carried in LLDP packets or add cross-domain detection TLVs to LLDP packets.

You can use the **lldp global cross-domain-detection enable** or **lldp cross-domain-detection** command to enable LLDP cross-domain detection for a port. If the **lldp cross-domain-detection** command is not configured for the port, the global setting (configured with the **lldp global cross-domain-detection enable** command) applies. If both commands are configured for the port, the port-specific setting (configured with the **lldp cross-domain-detection** command) applies.

## Procedure

1. Enter system view.  
**system-view**
2. Enable LLDP cross-domain detection globally.  
**lldp global cross-domain-detection enable**  
By default, LLDP cross-domain detection is disabled globally.
3. Enter Layer 2 Ethernet interface view.  
**interface** *interface-type* *interface-number*
4. Configure the domain ID for LLDP cross-domain detection.

```
lldp cross-domain-detection domain-id domain-id
```

By default, the domain ID is not configured for LLDP cross-domain detection.

5. Enable or disable LLDP cross-domain detection for the port.

```
lldp cross-domain-detection { enable | disable }
```

By default, the global setting (configured with the **lldp global cross-domain-detection enable** command) applies.

## Command reference

### lldp cross-domain-detection

Use **lldp cross-domain-detection** to enable or disable LLDP cross-domain detection for the port.

Use **undo cross-domain-detection** to restore the default.

#### Syntax

```
lldp cross-domain-detection { enable | disable }  
undo lldp cross-domain-detection
```

#### Default

The global setting (configured with the **lldp global cross-domain-detection enable** command) applies.

#### Views

Layer 2 Ethernet interface view

#### Predefined user roles

network-admin

#### Parameters

**enable**: Enables LLDP cross-domain detection for the port.

**disable**: Disables LLDP cross-domain detection for the port.

#### Usage guidelines

##### Operating mechanism

The LLDP cross-domain detection feature defines a private type of TLVs for LLDP, that is, the cross-domain detection TLVs. This TLV is used to advertise the local domain to the LLDP neighbor at the peer end. The LLDP cross-domain detection feature takes effect on a port only after you perform the following operations:

- Execute the **lldp global cross-domain-detection enable** or **lldp cross-domain-detection** command to enable LLDP cross-domain detection.
- Execute the **lldp cross-domain-detection domain-id** command to configure the domain ID for the local device.

Then, LLDP packets sent by the device will carry cross-domain detection TLVs.

A cross-domain detection TLV contains the domain ID, device bridge ID, port cost, and port ID. The device bridge ID is the bridge ID of the device that sends the cross-domain detection TLV. The port cost is the cost of the port that sends the cross-domain detection TLV. The port ID is the ID of the port that sends the cross-domain detection TLV.

Upon receiving LLDP packets carrying cross-domain detection TLVs, if the receiving ports are enabled with cross-domain detection, the device compares the domain IDs in the packets with the local setting:

- If the domain IDs are the same, the devices at the two ends of the LLDP session belong to the same domain, and the local device does not process the packets.
- If the domain IDs are different, the devices at the two ends of the LLDP session do not belong to the same domain. Data traffic transmission between each other might result in loops. To prevent this issue, the device performs the following operations:
  - If only one port receives an LLDP packet carrying the cross-domain detection TLV, the device blocks the port. In addition, it disables the port from receiving or sending any user data packets to eliminate loops in the network.
  - If multiple ports receive LLDP packets carrying the cross-domain detection TLVs with the same domain ID, the device compares the cross-domain detection TLVs received by the ports:
    - The cross-domain detection TLV received by the port with the smallest cost is the optimal TLV.
    - If the ports have the same cost, the cross-domain detection TLV received by the device with the smallest bridge ID is the optimal TLV.
    - If the devices have the same bridge ID, the cross-domain detection TLV received by the port with the smallest ID is the optimal TLV.

Except the port that receives the optimal cross-domain detection TLV, the device blocks all other ports that receive cross-domain detection TLVs. In addition, it disables the ports from receiving or sending any user data packets to eliminate loops in the network.

A blocked port can restore normal forwarding status when LLDP cross-domain detection is disabled or it receives a cross-domain detection TLV carrying the same domain ID as the local setting.

### Restrictions and guidelines

If the domain ID is not configured for LLDP cross-domain detection, or the port is not enabled with the cross-domain detection TLV advertisement capability, the cross-domain detection feature cannot take effect on the port. In this case, the device cannot identify cross-domain detection TLVs carried in LLDP packets or add cross-domain detection TLVs to LLDP packets.

You can use the **lldp global cross-domain-detection enable** or **lldp cross-domain-detection** command to enable LLDP cross-domain detection for a port. If the **lldp cross-domain-detection** command is not command for the port, the global setting (configured with the **lldp global cross-domain-detection enable** command) applies. If both commands are configured for the port, the port-specific setting (configured with the **lldp cross-domain-detection** command) applies.

### Examples

```
# Disable LLDP cross-domain detection for Ten-GigabitEthernet3/0/1.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] lldp cross-domain-detection disable
```

### Related commands

- **lldp cross-domain-detection domain-id**
- **lldp global cross-domain-detection enable**

### lldp cross-domain-detection domain-id

Use **lldp cross-domain-detection domain-id** to configure the domain ID for LLDP cross-domain detection.

Use `undo lldp cross-domain-detection domain-id` to remove the configuration.

## Syntax

```
lldp cross-domain-detection domain-id domain-id
undo lldp cross-domain-detection domain-id
```

## Default

The domain ID is not configured for LLDP cross-domain detection.

## Views

Layer 2 Ethernet interface view

## Predefined user roles

network-admin

## Parameters

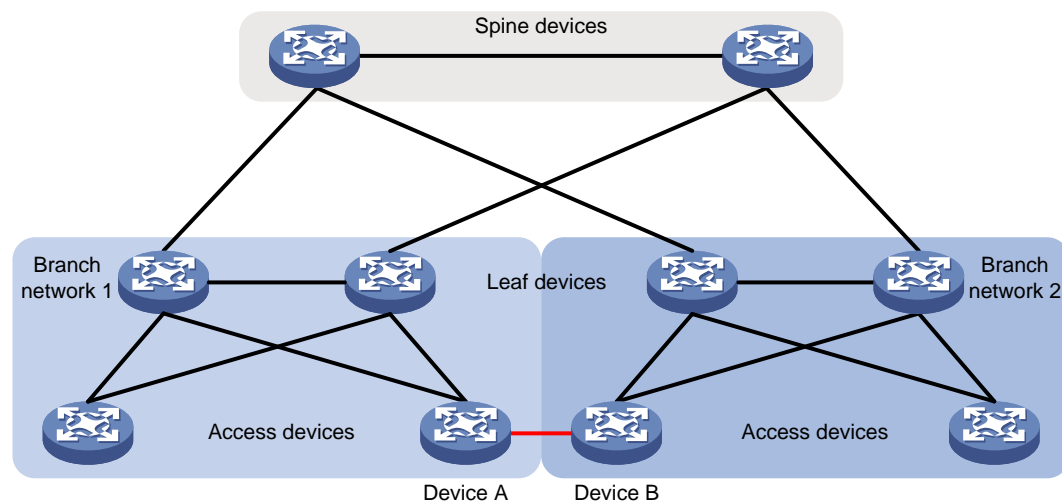
*domain-id*: Specifies a domain ID in the range of 1 to 10.

## Usage guidelines

### Application scenarios

As shown in Figure 4, Device A and Device B belongs to different branch networks. If a link exists between Device A and Device B, a loop might occur in the network. After configuring LLDP cross-domain detection, you can manually assign the devices to different domains, and use LLDP to detect whether the specified LLDP neighbor is in the local domain. In addition, you can block the link to neighbors in other domains to eliminate the potential loop risk.

**Figure 4 LLDP cross-domain detection application scenario**



### Operating mechanism

The LLDP cross-domain detection feature defines a private type of TLVs for LLDP, that is, the cross-domain detection TLVs. This TLV is used to advertise the local domain to the LLDP neighbor at the peer end. The LLDP cross-domain detection feature takes effect on a port only after you perform the following operations:

- Execute the `lldp global cross-domain-detection enable` or `lldp cross-domain-detection` command to enable LLDP cross-domain detection.
- Execute the `lldp cross-domain-detection domain-id` command to configure the domain ID for the local device.

Then, LLDP packets sent by the device will carry cross-domain detection TLVs.

A cross-domain detection TLV contains the domain ID, device bridge ID, port cost, and port ID. The device bridge ID is the bridge ID of the device that sends the cross-domain detection TLV. The port cost is the cost of the port that sends the cross-domain detection TLV. The port ID is the ID of the port that sends the cross-domain detection TLV.

Upon receiving LLDP packets carrying cross-domain detection TLVs, if the receiving ports are enabled with cross-domain detection, the device compares the domain IDs in the packets with the local setting:

- If the domain IDs are the same, the devices at the two ends of the LLDP session belong to the same domain, and the local device does not process the packets.
- If the domain IDs are different, the devices at the two ends of the LLDP session do not belong to the same domain. Data traffic transmission between each other might result in loops. To prevent this issue, the device performs the following operations:
  - If only one port receives an LLDP packet carrying the cross-domain detection TLV, the device blocks the port. In addition, it disables the port from receiving or sending any user data packets to eliminate loops in the network.
  - If multiple ports receive LLDP packets carrying the cross-domain detection TLVs with the same domain ID, the device compares the cross-domain detection TLVs received by the ports:
    - The cross-domain detection TLV received by the port with the smallest cost is the optimal TLV.
    - If the ports have the same cost, the cross-domain detection TLV received by the device with the smallest bridge ID is the optimal TLV.
    - If the devices have the same bridge ID, the cross-domain detection TLV received by the port with the smallest ID is the optimal TLV.

Except the port that receives the optimal cross-domain detection TLV, the device blocks all other ports that receive cross-domain detection TLVs. In addition, it disables the ports from receiving or sending any user data packets to eliminate loops in the network.

A blocked port can restore normal forwarding status when LLDP cross-domain detection is disabled or it receives a cross-domain detection TLV carrying the same domain ID as the local setting.

### Restrictions and guidelines

If the domain ID is not configured for LLDP cross-domain detection, or the port is not enabled with the cross-domain detection TLV advertisement capability, the cross-domain detection feature cannot take effect on the port. In this case, the device cannot identify cross-domain detection TLVs carried in LLDP packets or add cross-domain detection TLVs to LLDP packets.

### Examples

```
# Configure domain ID 2 for LLDP cross-domain detection on Ten-GigabitEthernet3/0/1.
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 3/0/1
[Sysname-Ten-GigabitEthernet3/0/1] lldp cross-domain-detection domain-id 2
```

### Related commands

- **lldp cross-domain-detection**
- **lldp global cross-domain-detection enable**

### lldp global cross-domain-detection enable

Use **lldp global cross-domain-detection enable** to enable LLDP cross-domain detection globally.

Use **undo lldp global cross-domain-detection enable** to disable LLDP cross-domain detection globally.

## Syntax

```
lldp global cross-domain-detection enable
undo lldp global cross-domain-detection enable
```

## Default

LLDP cross-domain detection is disabled globally.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

### Operating mechanism

The LLDP cross-domain detection feature defines a private type of TLVs for LLDP, that is, the cross-domain detection TLVs. This TLV is used to advertise the local domain to the LLDP neighbor at the peer end. The LLDP cross-domain detection feature takes effect on a port only after you perform the following operations:

- Execute the **lldp global cross-domain-detection enable** or **lldp cross-domain-detection** command to enable LLDP cross-domain detection.
- Execute the **lldp cross-domain-detection domain-id** command to configure the domain ID for the local device.

Then, LLDP packets sent by the device will carry cross-domain detection TLVs.

A cross-domain detection TLV contains the domain ID, device bridge ID, port cost, and port ID. The device bridge ID is the bridge ID of the device that sends the cross-domain detection TLV. The port cost is the cost of the port that sends the cross-domain detection TLV. The port ID is the ID of the port that sends the cross-domain detection TLV.

Upon receiving LLDP packets carrying cross-domain detection TLVs, if the receiving ports are enabled with cross-domain detection, the device compares the domain IDs in the packets with the local setting:

- If the domain IDs are the same, the devices at the two ends of the LLDP session belong to the same domain, and the local device does not process the packets.
- If the domain IDs are different, the devices at the two ends of the LLDP session do not belong to the same domain. Data traffic transmission between each other might result in loops. To prevent this issue, the device performs the following operations:
  - If only one port receives an LLDP packet carrying the cross-domain detection TLV, the device blocks the port. In addition, it disables the port from receiving or sending any user data packets to eliminate loops in the network.
  - If multiple ports receive LLDP packets carrying the cross-domain detection TLVs with the same domain ID, the device compares the cross-domain detection TLVs received by the ports:
    - The cross-domain detection TLV received by the port with the smallest cost is the optimal TLV.
    - If the ports have the same cost, the cross-domain detection TLV received by the device with the smallest bridge ID is the optimal TLV.
    - If the devices have the same bridge ID, the cross-domain detection TLV received by the port with the smallest ID is the optimal TLV.

Except the port that receives the optimal cross-domain detection TLV, the device blocks all other ports that receive cross-domain detection TLVs. In addition, it disables the ports from receiving or sending any user data packets to eliminate loops in the network.



A blocked port can restore normal forwarding status when LLDP cross-domain detection is disabled or it receives a cross-domain detection TLV carrying the same domain ID as the local setting.

### Restrictions and guidelines

If the domain ID is not configured for LLDP cross-domain detection, or the port is not enabled with the cross-domain detection TLV advertisement capability, the cross-domain detection feature cannot take effect on the port. In this case, the device cannot identify cross-domain detection TLVs carried in LLDP packets or add cross-domain detection TLVs to LLDP packets.

You can use the `lldp global cross-domain-detection enable` or `lldp cross-domain-detection` command to enable LLDP cross-domain detection for a port. If the `lldp cross-domain-detection` command is not command for the port, the global setting (configured with the `lldp global cross-domain-detection enable` command) applies. If both commands are configured for the port, the port-specific setting (configured with the `lldp cross-domain-detection` command) applies.

### Examples

```
# Enable LLDP cross-domain detection globally.
<Sysname> system-view
[Sysname] lldp global cross-domain-detection enable
```

### Related commands

- `lldp cross-domain-detection`
- `lldp cross-domain-detection domain-id`

## New feature: Using the subscriber ID as the client ID in all received DHCP requests

### Using the subscriber ID as the client ID in all received DHCP requests

#### About this task

Typically, after receiving a DHCP request on a client-facing interface, the DHCP server identifies the client by the **Client ID** or **chaddr** field in the DHCP request, and assigns an IP address to the client. When a new client is attached to the interface and requests an IP address, the DHCP server assigns a new IP address to the client, because the **Client ID** or **chaddr** field changes. In certain scenarios, such as industrial production lines, when a device attached to an industrial switch is replaced by another device, the new device needs to participate in services with the same IP address.

To meet this requirement, enable the DHCP server to use the subscriber ID as the client ID in all received DHCP requests.

With this feature enabled on a DHCP server interface, the DHCP server performs interface-based address assignment as follows: 1. Identifies all client IDs in the DHCP requests received on that interface as the subscriber ID. 2. Assigns IP addresses based on the subscriber ID (interface name), ensuring that clients attached to this interface share the same IP address.

You can enable this feature globally by using the `dhcp server subscriber-id replace client-id global` command, or on a per-interface basis by using the `dhcp server subscriber-id replace client-id` command.

- This feature is enabled on an interface as long as it is enabled globally or on the interface.

- To enable this feature only on a single interface, you must disable this feature globally, and then enable the feature on the desired interface by using the **dhcp server subscriber-id replace client-id** command.

## Procedure

1. Enter system view.  
**system-view**
2. Define the subscriber ID as interface name.  
**dhcp server subscriber-id interface-name**  
By default, content of the subscriber ID is not defined.
3. Enable the DHCP server to use the subscriber ID as the client ID on all interfaces.  
**dhcp server subscriber-id replace client-id global**  
By default, the DHCP server does not use the subscriber ID as the client ID.
4. Enable the DHCP server to use the subscriber ID as the client ID only on a single interface.
  - a. Globally disable the DHCP server from using the subscriber ID as the client ID.  
**undo dhcp server subscriber-id replace client-id global**  
By default, the DHCP server is globally disabled from using the subscriber ID as the client ID.
  - b. Enter interface view.  
**interface interface-type interface-number**
  - c. Enable the DHCP server to use the subscriber ID as the client ID on the interface.  
**dhcp server subscriber-id replace client-id**  
By default, the DHCP server to use the subscriber ID as the client ID on an interface.

## Command reference

### dhcp server subscriber-id replace client-id

Use **dhcp server subscriber-id replace client-id** to enable the DHCP server to use the subscriber ID as the client ID on an interface.

Use **undo dhcp server subscriber-id replace client-id** to disable the DHCP server from using the subscriber ID as the client ID on an interface.

#### Syntax

```
dhcp server subscriber-id replace client-id
undo dhcp server subscriber-id replace client-id
```

#### Default

The DHCP server does not use the subscriber ID as the client ID on any interface.

#### Views

Layer 2 Ethernet interface view/Layer 2 aggregate interface view

#### Predefined user roles

network-admin

#### Usage guidelines

##### Application scenarios

Typically, after receiving a DHCP request on a client-facing interface, the DHCP server identifies the client by the **Client ID** or **chaddr** field in the DHCP request, and assigns an IP address to the client. When a new client is attached to the interface and requests an IP address, the DHCP server assigns a new IP address to the client, because the **Client ID** or **chaddr** field changes. In certain scenarios, such as industrial production lines, when a device attached to an industrial switch is replaced by another device, the new device needs to participate in services with the same IP address.

To meet this requirement, enable the DHCP server to use the subscriber ID as the client ID in all received DHCP requests.

### Operating mechanism

With this feature enabled on a DHCP server interface, the DHCP server performs interface-based address assignment as follows: 1. Identifies all client IDs in the DHCP requests received on that interface as the subscriber ID. 2. Assigns IP addresses based on the subscriber ID (interface name), ensuring that clients attached to this interface share the same IP address.

### Prerequisites

To have this feature take effect, you must first define the subscriber ID as interface name by executing the **dhcp server subscriber-id interface-name** command.

## Examples

# Enable the DHCP server to use the subscriber ID as the client ID on an interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp server subscriber-id replace client-id
```

## dhcp server subscriber-id replace client-id global

Use **dhcp server subscriber-id replace client-id global** to enable the DHCP server to use the subscriber ID as the client ID on all interfaces.

Use **undo dhcp server subscriber-id replace client-id** to globally disable the DHCP server from using the subscriber ID as the client ID.

## Syntax

```
dhcp server subscriber-id replace client-id global
undo dhcp server subscriber-id replace client-id global
```

## Default

The DHCP server does not use the subscriber ID as the client ID on any interface.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

### Application scenarios

Typically, after receiving a DHCP request on a client-facing interface, the DHCP server identifies the client by the **Client ID** or **chaddr** field in the DHCP request, and assigns an IP address to the client. When a new client is attached to the interface and requests an IP address, the DHCP server assigns a new IP address to the client, because the **Client ID** or **chaddr** field changes. In certain scenarios, such as industrial production lines, when a device attached to an industrial switch is replaced by another device, the new device needs to participate in services with the same IP address.

To meet this requirement, enable the DHCP server to use the subscriber ID as the client ID in all received DHCP requests.

### Operating mechanism

With this feature enabled on a DHCP server interface, the DHCP server performs interface-based address assignment as follows: 1. Identifies all client IDs in the DHCP requests received on that interface as the subscriber ID. 2. Assigns IP addresses based on the subscriber ID (interface name), ensuring that clients attached to this interface share the same IP address.

You can enable this feature globally by using the **dhcp server subscriber-id replace client-id global** command, or on a per-interface basis by using the **dhcp server subscriber-id replace client-id** command.

- This feature is enabled on an interface as long as it is enabled globally or on the interface.
- To enable this feature only on a single interface, you must disable this feature globally, and then enable the feature on the desired interface by using the **dhcp server subscriber-id replace client-id** command.

### Prerequisites

To have this feature take effect, you must first define the subscriber ID as interface name by executing the **dhcp server subscriber-id interface-name** command.

### Examples

# Enable the DHCP server to use the subscriber ID as the client ID on all interfaces.

```
<Sysname> system-view
[Sysname] dhcp server subscriber-id replace client-id global
```

### dhcp server subscriber-id interface-name

Use **dhcp server subscriber-id interface-name** to define the subscriber ID as interface name.

Use **undo dhcp server subscriber-id replace client-id** to remove the configuration.

### Syntax

```
dhcp server subscriber-id interface-name
undo dhcp server subscriber-id interface-name
```

### Default

Content of the subscriber ID is not defined.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

Before enabling the DHCP server to use the subscriber ID as the client ID, you must use this command to define the subscriber ID as interface name. If you fail to do so, the DHCP server cannot perform interface-based address assignment and thus it cannot assign the same IP address to clients attached to the same interface.

### Examples

# Define the subscriber ID as interface name.

```
<Sysname> system-view
[Sysname] dhcp server subscriber-id interface-name
```

# New feature: Configuring resource monitoring

## Configuring resource monitoring

### About this task

The resource monitoring feature enables the device to monitor the available amounts of types of resources, for example, the space for ARP entries. The device samples the available amounts periodically and compares the samples with resource depletion thresholds to identify the resource depletion status.

The device supports a minor resource depletion threshold and a severe resource depletion threshold for each supported resource type.

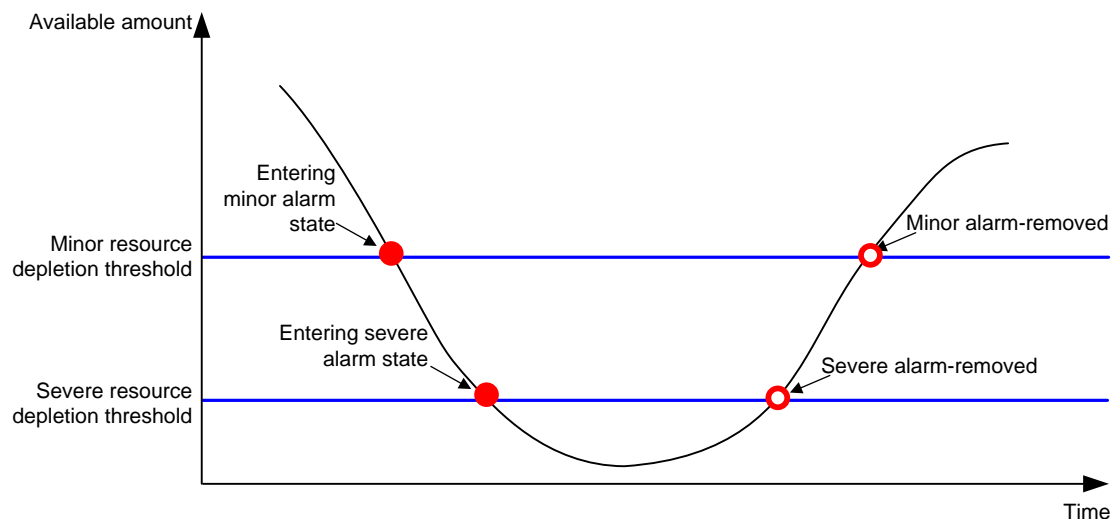
- If the available amount is equal to or less than the minor resource depletion threshold but greater than the severe resource depletion threshold, the resource type is in minor alarm state.
- If the available amount is equal to or less than the severe resource depletion threshold, the resource type is in severe alarm state.
- If the available amount increases above the minor resource depletion threshold, the resource type is in recovered state.

When a resource type enters severe alarm state, the device issues a severe alarm. If the resource type stays in severe alarm state, the device resends severe alarms periodically.

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

Resource depletion alarms can be sent to NETCONF, SNMP, and the information center to be encapsulated as NETCONF events, SNMP traps and informs, and log messages. For more information, see NETCONF, SNMP, and information center in *Network Management and Monitoring Configuration Guide*.

**Figure 1 Resource depletion alarms and alarm-removed notifications**



### Procedure

1. Enter system view.  
**system-view**

2. Set resource depletion thresholds.

```
resource-monitor resource resource-name slot slot-number cpu
cpu-number 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.

**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 arp
Minor alarms resending: Enabled
```

Slot 1:

| Resource | Minor (%) | Severe (%) | Free/Total (absolute) |
|----------|-----------|------------|-----------------------|
| arp      | 20        | 10         | 970/1019              |

**Table 2 Command output**

| Field                  | Description                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------|
| Minor alarms resending | Status of the minor resource depletion alarm resending feature, <b>Enabled</b> or <b>Disabled</b> . |
| Resource               | Monitored resource type.                                                                            |
| Minor (%)              | Minor resource depletion threshold, in percentage.                                                  |
| Severe (%)             | Severe resource depletion threshold, in percentage.                                                 |
| Free/Total (absolute)  | Numbers of available resources and total resources, in absolute values.                             |

## Related commands

```
resource-monitor minor resend enable
resource-monitor resource
```

## resource-monitor minor resend enable

Use **resource-monitor minor resend enable** to enable resending of minor resource depletion alarms.

Use **undo resource-monitor minor resend enable** to disable resending of minor resource depletion alarms.

## Syntax

```
resource-monitor minor resend enable
undo resource-monitor minor resend enable
```

## Default

Resending of minor resource depletion alarms is enabled.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

The resending period is fixed at 24 hours for a severe alarm and is fixed at 7 \* 24 hours for a minor alarm.

## Examples

```
# Enable resending of minor resource depletion alarms.
<Sysname> system-view
[Sysname] resource-monitor minor resend enable
```

## Related commands

```
display resource-monitor
resource-monitor output
resource-monitor resource
```

## resource-monitor output

Use **resource-monitor output** to specify destinations for resource depletion alarms.

Use **undo resource-monitor output** to remove destinations for resource depletion alarms.

## Syntax

```
resource-monitor output { netconf-event | snmp-notification | syslog } *
undo resource-monitor output [ netconf-event | snmp-notification | syslog ]
*
```

## Default

Resource depletion alarms are 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 3](#) shows the resource types that can be monitored.

**Table 3 Resource types that can be monitored**

| Resource type | Description                                                                 |
|---------------|-----------------------------------------------------------------------------|
| arp           | ARP resources.                                                              |
| ipv4host      | IPv4 host route resources after the UNI mode is enabled.                    |
| ipv4route     | Network routes and IPv4 host route resources not enabled with the UNI mode. |
| ipv6host      | IPv6 host route resources after the UNI mode is enabled.                    |
| ipv6route     | Network routes and IPv6 host route resources not enabled with the UNI mode. |
| nd            | ND resources.                                                               |
| nexthoppool1  | Next-hop pool resources for the underlay network.                           |

**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 on slot 1.
```

```
<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: Sending EAP-Success packets upon successful authorization in 802.1X

## Sending EAP-Success packets upon successful authorization

### About this task

The access device can send EAP-Success packets to 802.1X clients when it receives RADIUS Access-Accept packets from the RADIUS server upon successful authentication or authorization.

In the subnet authorization scenario, an 802.1X client must obtain an IP address through DHCP from the authorization subnet for network access after it receives an EAP-Success packet from the access device.

To make sure the 802.1X client can obtain an IP address from the authorization subnet, configure the access device to send EAP-Success packets upon successful authorization.

If the access device sends EAP-Success packets upon successful authentication, the client might send a DHCP request before it receives the authorization information. In this situation, the DHCP request is sent on the initial subnet to which the client is attached. The client will be unable to access the network with the IP address obtained from the initial subnet after the authorization subnet is issued.

### Restrictions and guidelines

When you configure the device to send EAP-Success packets upon successful authorization, evaluate its impact on authentication service. When a large number of authentication sessions are present, this setting might result in authentication failure because the RADIUS server or access device fails to return EAP-Success packets before the authentication timeout time expires.

### Procedure

1. Enter system view.

```
system-view
```

2. Configure the device to send EAP-Success packets to clients upon successful authorization.

```
dot1x eap-success post-authorization
```

By default, the device sends EAP-Success packets to clients upon successful authentication.

# Command reference

## dot1x eap-success post-authorization

Use `dot1x eap-success post-authorization` to configure the device to send EAP-Success packets to clients upon successful authorization.

Use `undo dot1x eap-success post-authorization` to configure the device to send EAP-Success packets to clients upon successful authentication.

### Syntax

```
dot1x eap-success post-authorization
```

```
undo dot1x eap-success post-authorization
```

### Default

The device sends EAP-Success packets to clients upon successful authentication.

### Views

System view

### Default command level

network-admin

### Usage guidelines

#### Application scenarios

The access device can send EAP-Success packets to 802.1X clients when it receives RADIUS Access-Accept packets from the RADIUS server upon successful authentication or authorization.

In the subnet authorization scenario, an 802.1X client must obtain an IP address through DHCP from the authorization subnet for network access after it receives an EAP-Success packet from the access device.

To make sure the 802.1X client can obtain an IP address from the authorization subnet, configure the access device to send EAP-Success packets upon successful authorization.

If the access device sends EAP-Success packets upon successful authentication, the client might send a DHCP request before it receives the authorization information. In this situation, the DHCP request is sent on the initial subnet to which the client is attached. The client will be unable to access the network with the IP address obtained from the initial subnet after the authorization subnet is issued.

#### Restrictions and guidelines

When you configure the device to send EAP-Success packets upon successful authorization, evaluate its impact on authentication service. When a large number of authentication sessions are present, this setting might result in authentication failure because the RADIUS server or access device fails to return EAP-Success packets before the authentication timeout time expires.

### Examples

# Configure the device to send EAP-Success packets to clients upon successful authorization.

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

```
[Sysname] dot1x eap-success post-authorization
```

# Modified feature: Support for specifying a custom hexadecimal string as the content of the Remote ID sub-option

## Feature change description

As from this release, you can configure a custom hexadecimal string as the content of the Remote ID sub-option on the DHCP snooping device or the DHCP relay agent.

## Command changes

### Modified command: dhcp snooping information remote-id

#### Old syntax

```
dhcp snooping information remote-id { normal [ format { ascii | hex } ] |  
[ vlan vlan-id ] { string remote-id | sysname } }  
  
undo dhcp snooping information remote-id [ vlan vlan-id ]
```

#### New syntax

```
dhcp snooping information remote-id { normal [ format { ascii | hex } ] |  
[ vlan vlan-id ] { hex hex-string | string remote-id | sysname } }  
  
undo dhcp snooping information remote-id [ vlan vlan-id ]
```

#### Views

Layer 2 Ethernet interface view/Layer 2 aggregate interface view

VLAN view

---

**NOTE:**

VLAN view is supported only in Release 6350 and later.

---

## Change description

Before modification: The device only supports using a custom string as the content of the Remote ID sub-option. The string cannot be hexadecimal.

After modification: The device supports using a custom hexadecimal string as the content of the Remote ID sub-option.

#### Parameters

**hex** *hex-string*: Specifies a hexadecimal string as the content of the Remote ID sub-option. The string length must be an even integer in the range of 2 to 256.

### Modified command: dhcp relay information remote-id

#### Old syntax

```
dhcp relay information remote-id { normal [ format { ascii | hex } ] | string  
remote-id | sysname }  
  
undo dhcp relay information remote-id
```

## New syntax

```
dhcp relay information remote-id { hex remote-id | normal [ format { ascii  
| hex } ] | string remote-id | sysname }  
undo dhcp relay information remote-id
```

## Views

Interface view

## Change description

Before modification: The device only supports using a custom string as the content of the Remote ID sub-option. The string cannot be hexadecimal.

After modification: The device supports using a custom hexadecimal string as the content of the Remote ID sub-option.

## Parameters

**hex** *hex-string*: Specifies a hexadecimal string as the content of the Remote ID sub-option. The string length must be an even integer in the range of 2 to 256.

# Modified feature: Support for specifying a custom ASCII string as the client ID of a static binding

## Feature change description

As from this release, when you configure a static binding in a DHCP address pool, you can specify a custom ASCII string as the client ID of that static binding.

## Modified command: static-bind

### Old syntax

```
static-bind ip-address ip-address [ mask-length | mask mask ]  
{ client-identifier client-identifier | hardware-address  
hardware-address [ ethernet | token-ring ] }  
undo static-bind ip-address ip-address
```

### New syntax

```
static-bind ip-address ip-address [ mask-length | mask mask ]  
{ client-identifier { ascii ascii-string | hex hex-string } |  
hardware-address hardware-address [ ethernet | token-ring ] }  
undo static-bind ip-address ip-address
```

## Views

DHCP address pool view

## Change description

Before modification: You can use the **client-identifier** *client-identifier* option to specify a client ID and the client ID is a hexadecimal string.

After modification: The *client-identifier* argument is replaced by the **hex** *hex-string* and **ascii** *ascii-string* options. The **hex** *hex-string* option specifies a hexadecimal client ID and the **ascii** *ascii-string* option specifies an ASCII client ID.

## Parameters

**hex** *hex-string*: Specifies a hexadecimal string of 4 to 254 characters as the client ID. The string can contain only hexadecimal numbers and hyphen (-), in the format of H-H-H.... The last H can be a two-digit or four-digit hexadecimal number while the other Hs must be all four-digit hexadecimal numbers. For example, aabb-cccc-dd is valid, and aabb-c-dddd and aabb-cc-dddd are invalid.

**ascii** *ascii-string*: Specifies an ASCII string of 1 to 127 characters as the client ID.

# Release 6351P02

This release has no feature changes.

# Release 6351

This release has the following changes:

- New feature: Advertising proprietary TLVs on an interface
- New feature: Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection
- New feature: Loopback test on an interface
- New feature: Configuring disk usage monitoring
- New feature: Enabling the portal fail-permit feature for portal Web servers
- New feature: Configuring packet detection for 802.1X authentication
- New feature: Configuring packet detection for MAC authentication
- New feature: Specifying an IP address and mask for calculating the source IP of ARP detection packets
- New feature: Associating PoE with Track
- New feature: many-to-one VLAN mapping
- New feature: Disabling receiving a specific type of ICMP messages
- New feature: Disabling sending a specific type of ICMP messages
- New feature: MAC swap loopback test configuration
- New feature: Configuring the TMPDO for the MPS
- New feature: Configuring port collaboration
- New feature: Disabling PoE power supply on shutdown interfaces
- New feature: Configuring PoE delay
- New feature: Setting the PoE guard band
- New feature: Configuring a PD disconnection detection mode
- New feature: Ignoring the PD power class
- Modified feature: Applying a portal Web server to an interface
- Modified feature: Displaying portal configuration and running information on an interface
- Modified feature: Display power supply information
- Modified feature: Configuring the padding mode and padding format for the Circuit ID sub-option in VLAN view
- Modified feature: Enabling DHCP snooping to support Option 82 in VLAN view
- Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option in VLAN view
- Modified feature: Configuring the Option 82 handling strategy for DHCP request messages in VLAN view
- Modified feature: Configuring the padding mode for the Vendor-Specific sub-option in VLAN view
- Modified feature: Changing the default settings for outputting port state transition information
- Modified feature: Support of 10G fiber ports for 2.5G transceiver modules
- Modified feature: PD detection mode
- Modified feature: Enabling recording user IP address conflicts
- Modified feature: Enabling IP conflict notification



- [Modified feature: Testing the cable connection of an Ethernet interface](#)
- [Modified feature: Allowing inrush currents of PDs](#)

## New feature: Advertising proprietary TLVs on an interface

### Advertising proprietary TLVs on an interface

As from this version, proprietary TLVs can be advertised on an interface. Only actual power TLVs are supported. This type of TLVs provides PoE power information about an interface for the peer to obtain the actual power that can be provided by the local.

### Command reference

#### lldp tlv-enable private-tlv

Use **lldp tlv-enable private-tlv** to specify types of proprietary TLVs advertisable on an interface.

Use **undo lldp tlv-enable private-tlv** to disabling advertising proprietary TLVs on an interface.

#### Syntax

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-enable
private-tlv actual-power

undo lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-enable
private-tlv actual-power
```

#### Default

No proprietary TLVs can be advertised on an interface.

#### Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

#### Predefined user roles

network-admin

#### Parameters

**agent**: Specifies an agent type. If you do not specify an agent type, the command specifies types of proprietary TLVs that can be advertised by nearest bridge agents.

**nearest-customer**: Specifies nearest customer bridge agents.

**nearest-nontpmr**: Specifies nearest non-TPMR bridge agents.

**actual-power**: Specifies actual power TLVs.

#### Usage guidelines

proprietary TLVs are used to meet specific transmission requirements on network management. Other vendors cannot identify proprietary TLVs carried in LLDPDUs.

Only actual power TLVs are supported in the current software version. This type of TLVs provides PoE power information about an interface.

## Examples

```
# Configure nearest customer bridge agents to advertise actual power TLVs on interface
GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable private-tlv
actual-power
```

## New feature: Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection

### Configuring a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection

#### About this task

Perform this task to ensure that a dynamic aggregation group selects a high-speed member port as the reference port. After you perform this task, the reference port will be selected based on the criteria in order of device ID, port speed, and port ID.

#### Restrictions and guidelines

Changing reference port selection criteria might cause transient traffic interruption. Make sure you understand the impact of this task on your network.

You must perform this task at both ends of the aggregate link so the peer aggregation systems use the same criteria for reference port selection.

As a best practice, shut down the peer aggregate interfaces before you execute this command and bring up the interfaces after this command is executed on both of them.

#### Procedure

1. Enter system view.  
**system-view**
2. Enter Layer 2 aggregate interface view.  
**interface bridge-aggregation** *interface-number*
3. Specify port speed as the prioritized criterion for reference port selection.  
**lACP select speed**

By default, port ID is the prioritized criterion for reference port selection of a dynamic aggregation group.

## Command reference

### lACP select speed

Use **lACP select speed** to configure a dynamic aggregation group to use port speed as the prioritized criterion for reference port selection.

Use **undo lACP select speed** to restore the default.

## Syntax

```
lacp select speed
undo lacp select speed
```

## Default

Port ID is the prioritized criterion for reference port selection in a dynamic aggregation group.

## Views

Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Usage guidelines



### CAUTION:

Changing reference port selection criteria might cause transient traffic interruption. When you use this command, make sure you understand its impact on your network.

This command enables a dynamic aggregation group to select a high-speed member port as the reference port.

You must execute this command at both ends of the aggregate link so the peer aggregation systems use the same criteria for reference port selection.

As a best practice, shut down the peer aggregate interfaces before you execute this command and bring up the interfaces after this command is executed on both of them.

This command takes effect only on dynamic aggregate interfaces. On a static aggregate interface, you can execute this command, but the setting cannot take effect.

## Examples

# Specify port speed as the prioritized criterion for reference port selection on Layer 2 dynamic aggregate interface Bridge-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation1] lacp select speed
```

# New feature: Loopback test on an interface

## Performing a loopback test on an interface

### About this task

Perform this task to determine whether an Ethernet link works correctly. Loopback tests includes the following types:

- **Internal loopback test**—Tests the device where the Ethernet interface resides. The Ethernet interface sends outgoing packets back to the local device. If the device fails to receive the packets, the device fails.
- **External loopback test**—Tests the inter-device link. The Ethernet interface sends incoming packets back to the remote device. If the remote device fails to receive the packets, the inter-device link fails.

## Restrictions and guidelines

The **shutdown**, **port up-mode**, **loopback**, and **loopback-test** commands are mutually exclusive on an interface.

## Procedure

1. Enter system view.  
**system-view**
2. Enter Ethernet interface view.  
**interface** *interface-type interface-number*
3. Perform a loopback test.  
**loopback-test**{ **external** | **internal** }

## Command reference

### New command: loopback-test

Use **loopback-test** to perform a loopback test.

#### Syntax

```
loopback-test { external | internal }
```

#### Views

Ethernet interface view

#### Predefined user roles

network-admin

#### Parameters

**external**: Performs an external loopback test.

**internal**: Performs an internal loopback test.

#### Usage guidelines

The **shutdown**, **port up-mode**, **loopback**, and **loopback-test** commands are mutually exclusive on an interface.

#### Examples

```
# Perform an internal loopback test on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-test internal
```

## New feature: Configuring disk usage monitoring

### About this task

This feature enables the device to periodically sample the usage of a disk and compare the usage with the threshold. If the disk usage exceeds the threshold, the device sends a high disk

usage alarm to the NETCONF module. For more information about the NETCONF module, see *Network Management and Monitoring Configuration Guide*.

## Procedure

1. Enter system view.  
**system-view**
2. Set the disk usage sampling interval.  
**monitor disk-usage interval** *interval*  
By default, the disk usage sampling interval is 300 seconds.
3. Set the usage threshold for a disk.  
**monitor disk-usage [ slot slot-number ] disk disk-name threshold**  
*threshold-value*  
By default, the disk usage threshold is 95%.

## Command changes

### monitor disk-usage disk

Use **monitor disk-usage disk** to set the usage threshold for a disk.

Use **undo monitor disk-usage disk** to restore the default.

### Syntax

```
monitor disk-usage [ slot slot-number ] disk disk-name threshold  
threshold-value  
undo monitor disk-usage [ slot slot-number ] disk disk-name threshold
```

### Default

By default, the disk usage threshold is 95%.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**slot** *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command applies to the master device.

**disk** *disk-name*: Specifies a storage medium by its name. This option is case sensitive. The system will prompt a parameter error if you enter this option incorrectly.

**threshold** *threshold-value*: Specifies the disk usage threshold in percentage, in the range of 1 to 100.

### Usage guidelines

After you configure the usage threshold for a disk, the device compares the usage of the disk with the threshold at each sampling. If the usage exceeds the threshold, the device sends a high disk usage alarm to the NETCONF module. For more information about the NETCONF module see *Network Management and Monitoring Configuration Guide*.

### Examples

# Set the disk usage threshold to 80% for a storage medium.

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

```
[Sysname] monitor disk-usage disk flash threshold 80
```

## Related commands

```
monitor disk-usage interval
```

## monitor disk-usage interval

Use **monitor disk-usage interval** to set the disk usage sampling interval.

Use **undo monitor disk-usage interval** to restore the default.

## Syntax

```
monitor disk-usage interval interval
```

```
undo monitor disk-usage interval
```

## Default

The disk usage sampling interval is 300 seconds.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**interval** *interval-time*: Specifies the disk usage sampling interval in seconds, a multiple of five in the range of 5 to 1800.

## Usage guidelines

After you set the disk usage sampling interval, the device samples disk usages at the specified intervals.

## Examples

```
# Set the disk usage sampling interval to 120 seconds.
```

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

```
[Sysname] monitor disk-usage interval 120
```

## Related commands

```
monitor disk-usage disk
```

# New feature: Enabling the portal fail-permit feature for portal Web servers

## Enabling the portal fail-permit feature for portal Web servers

### About this task

You can configure the portal fail-permit feature on an interface. When the access device detects that the portal authentication server or portal Web server is unreachable, it allows users to have network access without portal authentication.

If you enable fail-permit for both the portal authentication server and the portal Web servers, the device does the following:

- Disables portal authentication when the portal authentication server is unreachable or all the portal Web servers are unreachable.
- Resumes portal authentication when both the portal authentication and Web servers are reachable.

After portal authentication resumes, unauthenticated users must pass portal authentication to access the network. Users who have passed portal authentication before the fail-permit event can continue accessing the network.

## Procedure

1. Enter system view.  
**system-view**
  2. Enter Layer 3 interface view.  
**interface** *interface-type* *interface-number*
  3. Enable portal fail-permit for portal Web servers on the interface.  
**portal [ ipv6 ] fail-permit web-server**
- By default, portal fail-permit is disabled for portal Web servers on an interface.

## Command reference

### portal fail-permit web-server

Use **portal fail-permit web-server** to enable the portal fail-permit feature for portal Web servers.

Use **undo portal fail-permit web-server** to disable the portal fail-permit feature for portal Web servers.

### Syntax

```
portal [ ipv6 ] fail-permit web-server
undo portal [ ipv6 ] fail-permit web-server
```

### Default

Portal fail-permit is disabled for portal Web servers.

### Views

Interface view

### Predefined user roles

network-admin

### Parameters

**ipv6**: Specifies IPv6 portal Web servers. To specify IPv4 portal Web servers, do not specify this keyword.

### Usage guidelines

On an interface enabled with portal fail-permit for a portal authentication server and portal Web servers, portal authentication on the interface is disabled in either of the following conditions:

- All portal Web servers are unreachable.
- The specified portal authentication server is unreachable.

Portal authentication resumes on the interface when the specified portal authentication server and a minimum of one portal Web server becomes reachable. After portal authentication resumes,

unauthenticated portal users need to pass authentication to access network resources. Portal users who have passed authentication can continue accessing network resources.

### Examples

```
# Enable portal fail-permit for the portal Web servers on VLAN-interface 100.
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal fail-permit web-server
```

### Related commands

```
display portal
```

## New feature: Configuring packet detection for 802.1X authentication

### Configuring packet detection for 802.1X authentication

#### About this task

When packet detection for 802.1X authentication is enabled on a port, the device sends detection packets to 802.1X users connected to that port at offline detection intervals set by using the offline detect timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

When packet detection for 802.1X authentication and 802.1X offline detection are both enabled, the device processes an 802.1X user as follows:

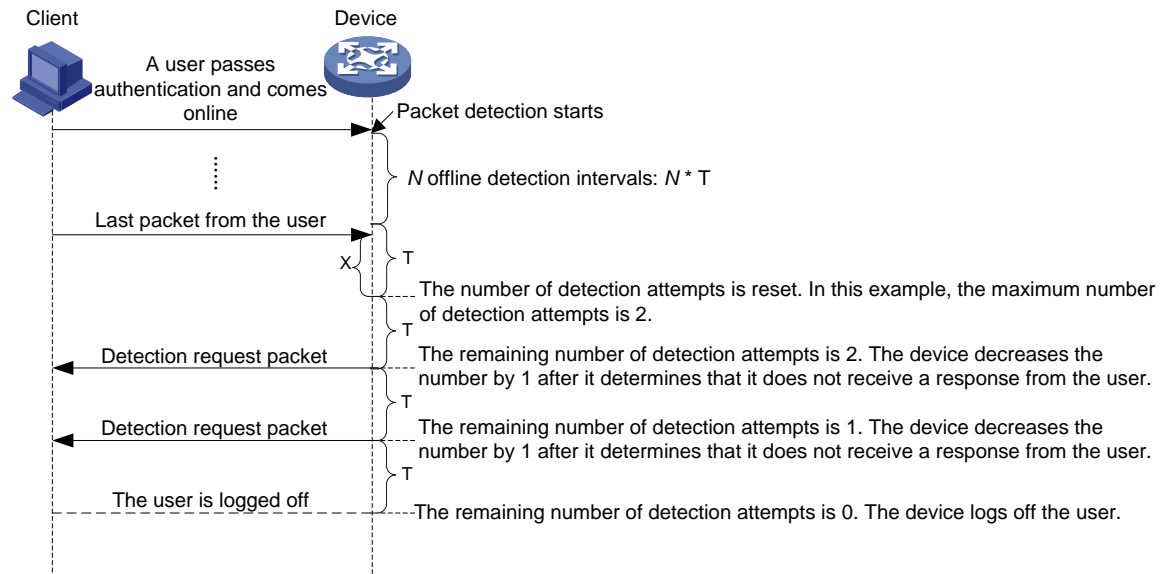
- If 802.1X offline detection determines that a user is online, the device does not send detection packets to that user.
- If 802.1X offline detection determines that a user is offline, the device does not immediately log off that user. Instead, the device sends a detection packet to that user. It will log off that user if it does not receive a response from that user after it has made the maximum packet transmission attempts within an offline detection interval.

802.1X uses ARP request packets to detect the online status of IPv4 users and uses NS packets to detect the online status of IPv6 users.

Packet detection adopts the principle of counting prior to judging. The device decreases the detection attempts (packet transmission attempts) by 1 only after it determines that it does not receive a response from a user. The device stops the detection process when the number of detection attempts becomes 0. The duration from the time when the user sends the last packet to the time when the user is logged off is calculated by using the following formula:  $\text{duration} = (\text{retries} + 1) * T + X$ . [Figure 1](#) shows the packet detection process. In this example, the device sends a detection packet to an 802.1X user for a maximum of two times.



**Figure 1 Network diagram for packet detection process**



The duration from the time when the user sends the last packet to the time when the user is logged off equals to  $3 * T + X$ .

## Restrictions and guidelines

To ensure that the device is aware of user IP address changes, enable ARP snooping and ND snooping in conjunction with packet detection for 802.1X authentication. If you do not enable ARP snooping or ND snooping, the device is unaware of user IP address changes. As a result, the device still sends detection packets to the users' original IP addresses and falsely log off these users.

## Procedure

1. Enter system view.  
**system-view**
2. Set the offline detect timer.  
**dot1x timer offline-detect** *offline-detect-value*  
By default, the offline detect timer expires in 300 seconds.
3. Enter interface view.  
**interface** *interface-type* *interface-number*
4. Enable packet detection for 802.1X authentication.  
**dot1x packet-detect enable**  
By default, packet detection for 802.1X authentication is disabled.
5. Set the maximum number of attempts for sending a detection packet to an 802.1X user.  
**dot1x packet-detect retry** *retries*  
By default, the device sends a detection packet to an 802.1X user for a maximum of two times.

## Command reference

### New command: dot1x packet-detect enable

Use **dot1x packet-detect enable** to enable packet detection for 802.1X authentication.

Use **undo dot1x packet-detect enable** to restore the default.

## Syntax

```
dot1x packet-detect enable
undo dot1x packet-detect enable
```

## Default

Packet detection for 802.1X authentication is disabled.

## Views

Layer 2 Ethernet interface view

## Predefined user roles

network-admin

## Usage guidelines

When packet detection for 802.1X authentication is enabled on a port, the device sends detection packets to 802.1X users connected to that port at offline detection intervals set by using the offline detect timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

When packet detection for 802.1X authentication and 802.1X offline detection are both enabled, the device processes an 802.1X user as follows:

- If 802.1X offline detection determines that a user is online, the device does not send detection packets to that user.
- If 802.1X offline detection determines that a user is offline, the device does not immediately log off that user. Instead, the device sends a detection packet to that user. It will log off that user if it does not receive a response from that user after it has made the maximum packet transmission attempts within an offline detection interval.

To ensure that the device is aware of user IP address changes, enable ARP snooping and ND snooping in conjunction with packet detection for 802.1X authentication. If you do not enable ARP snooping or ND snooping, the device is unaware of user IP address changes. As a result, the device still sends detection packets to the users' original IP addresses and falsely log off these users.

## Examples

```
# Enable packet detection for 802.1X authentication.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x packet-detect enable
```

## Related commands

```
dot1x timer offline-detect
port-security packet-detect arp-source-ip factor
dot1x packet-detect retry
```

## New command: dot1x packet-detect retry

Use **dot1x packet-detect retry** to set the maximum number of attempts for sending a detection packet to an 802.1X user.

Use **undo dot1x packet-detect retry** to restore the default.

## Syntax

```
dot1x packet-detect retry retries
undo dot1x packet-detect retry
```

## Default

The device sends a detection packet to an 802.1X user for a maximum of two times.

## Views

Layer 2 Ethernet interface view

## Predefined user roles

network-admin

## Parameters

*retries*: Sets the maximum number of attempts for sending a detection packet to an 802.1X user. The value range is 1 to 10.

## Usage guidelines

When packet detection for 802.1X authentication is enabled on a port, the device sends detection packets to 802.1X users connected to that port at offline detection intervals set by using the offline detect timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

If the device fails to send a detection packet to an 802.1X user because it does not obtain the IP address of that user when that user just comes online, the device still decreases the maximum packet transmission attempts by 1. To prevent an 802.1X user from being logged off because the device does not obtain the IP address of that user when that user just comes online, the device increases the maximum number of packet transmission attempts by 10 on the basis of the original configuration.

## Examples

# Set the maximum number of attempts to 8 for sending a detection packet to an 802.1X user.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x packet-detect retry 8
```

## Related commands

**dot1x packet-detect enable**

## Modified command: display dot1x connection

### Syntax

```
display dot1x connection [ open ] [ interface interface-type
interface-number | slot slot-number | user-mac mac-address | user-name
name-string ]
```

### Views

Any view

### Change description

Packet detection fields were added to the command output. The following information shows a sample command output:

# Display information about all online 802.1X users.

```
<Sysname> display dot1x connection
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: aaa
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
AAA authentication method: Local
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100

Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 2 s
Packet detection:
  Max attempts: 5
  Remaining attempts: 3
  Source IPv4 address: 192.168.1.3
  Source IPv4 mask: 255.255.0.0
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s
```

## New feature: Configuring packet detection for MAC authentication

### Configuring packet detection for MAC authentication

#### About this task

When packet detection for MAC authentication is enabled on a port, the device sends detection packets to MAC authentication users connected to that port at offline detection intervals set by using the offline detect timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

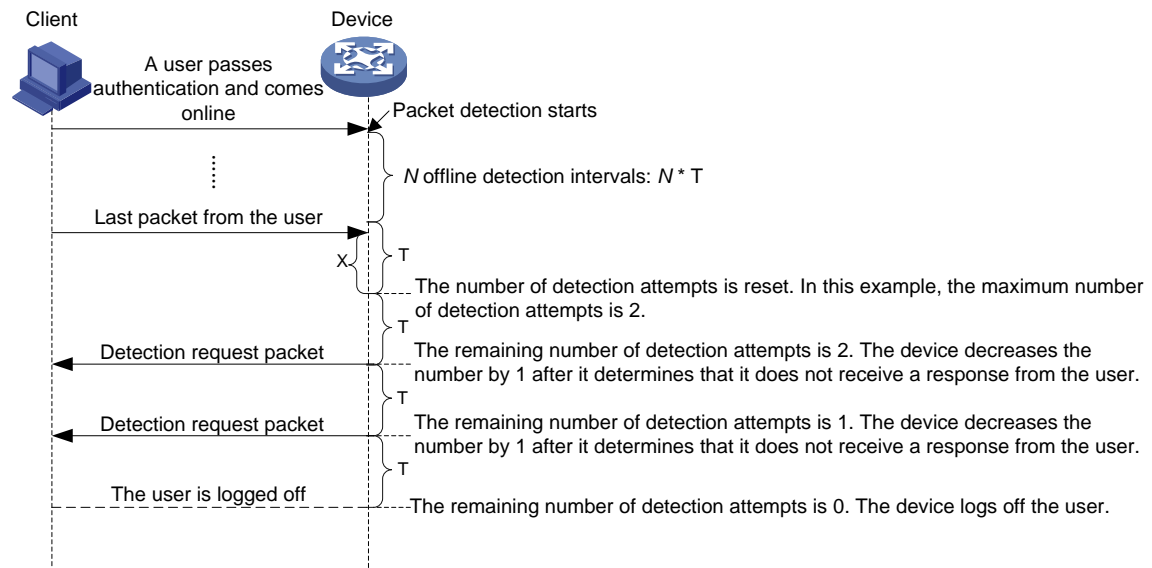
When packet detection for MAC authentication and MAC authentication offline detection are both enabled, the device processes a MAC authentication user as follows:

- If MAC authentication offline detection determines that a user is online, the device does not send detection packets to that user.
- If MAC authentication offline detection determines that a user is offline, the device does not immediately log off that user. Instead, the device sends a detection packet to that user. It will log off that user if it does not receive a response from that user after it has made the maximum packet transmission attempts within an offline detection interval.

MAC authentication uses ARP request packets to detect the online status of IPv4 users and uses NS packets to detect the online status of IPv6 users.

Packet detection adopts the principle of counting prior to judging. The device decreases the detection attempts (packet transmission attempts) by 1 only after it determines that it does not receive a response from a user. The device stops the detection process when the number of detection attempts becomes 0. The duration from the time when the user sends the last packet to the time when the user is logged off is calculated by using the following formula:  $\text{duration} = (\text{retries} + 1) * T + X$ . Figure 2 shows the packet detection process. In this example, the device sends a detection packet to a MAC authentication user for a maximum of two times.

**Figure 2 Network diagram for packet detection process**



The duration from the time when the user sends the last packet to the time when the user is logged off equals to  $3 * T + X$ .

## Restrictions and guidelines

To ensure that the device is aware of user IP address changes, enable ARP snooping and ND snooping in conjunction with packet detection for MAC authentication. If you do not enable ARP snooping or ND snooping, the device is unaware of user IP address changes. As a result, the device still sends detection packets to the users' original IP addresses and falsely log off these users.

## Procedure

1. Enter system view.  
**system-view**
2. Set the offline detect timer.  
**mac-authentication timer offline-detect** *offline-detect-value*  
By default, the offline detect timer expires in 300 seconds.
3. Enter interface view.  
**interface** *interface-type interface-number*
4. Enable packet detection for MAC authentication.  
**mac-authentication packet-detect enable**  
By default, packet detection for MAC authentication is disabled.
5. Set the maximum number of attempts for sending a detection packet to a MAC authentication user.  
**mac-authentication packet-detect retry** *retries*

By default, the device sends a detection packet to a MAC authentication user for a maximum of two times.

## Command reference

### New command: mac-authentication packet-detect enable

Use **mac-authentication packet-detect enable** to enable packet detection for MAC authentication.

Use **undo mac-authentication packet-detect enable** to restore the default.

#### Syntax

```
mac-authentication packet-detect enable
undo mac-authentication packet-detect enable
```

#### Default

Packet detection for MAC authentication is disabled.

#### Views

Layer 2 Ethernet interface view

#### Predefined user roles

network-admin

#### Usage guidelines

When packet detection for MAC authentication is enabled on a port, the device sends detection packets to MAC authentication users connected to that port at offline detection intervals set by using the offline detect timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

When packet detection for MAC authentication and MAC authentication offline detection are both enabled, the device processes a MAC authentication user as follows:

- If MAC authentication offline detection determines that a user is online, the device does not send detection packets to that user.
- If MAC authentication offline detection determines that a user is offline, the device does not immediately log off that user. Instead, the device sends a detection packet to that user. It will log off that user if it does not receive a response from that user after it has made the maximum packet transmission attempts within an offline detection interval.

MAC authentication uses ARP request packets to detect the online status of IPv4 users and uses NS packets to detect the online status of IPv6 users.

To ensure that the device is aware of user IP address changes, enable ARP snooping and ND snooping in conjunction with packet detection for MAC authentication. If you do not enable ARP snooping or ND snooping, the device is unaware of user IP address changes. As a result, the device still sends detection packets to the users' original IP addresses and falsely log off these users.

#### Examples

```
# Enable packet detection for MAC authentication on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication packet-detect enable
```

#### Related commands

```
mac-authentication timer offline-detect
```

```
port-security packet-detect arp-source-ip factor
mac-authentication packet-detect retry
```

## New command: mac-authentication packet-detect retry

Use **mac-authentication packet-detect retry** to set the maximum number of attempts for sending a detection packet to a MAC authentication user.

Use **undo mac-authentication packet-detect retry** to restore the default.

### Syntax

```
mac-authentication packet-detect retry retries
undo mac-authentication packet-detect retry
```

### Default

The device sends a detection packet to a MAC authentication user for a maximum of two times.

### Views

Layer 2 Ethernet interface view

### Predefined user roles

network-admin

### Parameters

*retries*: Sets the maximum number of attempts for sending a detection packet to a MAC authentication user. The value range is 1 to 10.

### Usage guidelines

When packet detection for MAC authentication is enabled on a port, the device sends detection packets to MAC authentication users connected to that port at offline detection intervals set by using the offline detect timer. If the device does not receive a response from a user after it has made the maximum packet transmission attempts within an offline detection interval, it logs off that user and requests the RADIUS server to stop accounting for the user.

To prevent a MAC authentication user from being logged off because the device does not obtain the IP address of that user when that user just comes online, the device increases the maximum number of packet transmission attempts by 10 on the basis of the original configuration.

### Examples

# On GigabitEthernet 1/0/1, set the maximum number of attempts to 8 for sending a detection packet to a MAC authentication user.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication packet-detect retry 8
```

### Related commands

```
mac-authentication packet-detect enable
```

## 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

Packet detection fields were added to the command output. The following information shows a sample command output:

# Display information about all online MAC authentication users.

```
<Sysname> display mac-authentication connection
```

```
Total connections: 1
```

```
Slot ID: 0
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```
User access state: Successful
```

```
Authentication domain: macusers
```

```
IPv4 address: 192.168.1.1
```

```
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
```

```
Initial VLAN: 1
```

```
Authorization untagged VLAN: 100
```

```
Authorization tagged VLAN: N/A
```

```
Authorization VSI: N/A
```

```
Authorization ACL number/name: 3001
```

```
Authorization dynamic ACL name: N/A
```

```
Authorization user profile: N/A
```

```
Authorization CAR: N/A
```

```
Authorization URL: N/A
```

```
Termination action: Radius-request
```

```
Session timeout period: 2 sec
```

```
Offline detection: 100 sec (server-assigned)
```

```
Packet detection:
```

```
Max attempts: 5
```

```
Remaining attempts: 3
```

```
Source IPv4 address: 192.168.1.3
```

```
Source IPv4 mask: 255.255.0.0
```

```
Online from: 2013/03/02 13:14:15
```

```
Online duration: 0h 2m 15s
```

## New feature: Specifying an IP address and mask for calculating the source IP of ARP detection packets

### Specifying an IP address and mask for calculating the source IP of ARP detection packets

#### About this task

By default, the device uses 0.0.0.0 as the source IP address of ARP detection packets. The network might have users that cannot respond to ARP detection packets with source IP address 0.0.0.0. As a result, the device inadequately determines that these users have gone offline. To resolve the issue,



use this feature to specify an IP address and mask for calculating the source IP of ARP detection packets sent to a user in conjunction with the user's IP address.

The device uses the following formula to calculate the source IP address of ARP detection packets: source IP = (user IP & specified mask) | (specified IP & ~specified mask). The ~mask parameter represents the reverse of a mask. For example, the reverse mask of 255.255.255.0 is 0.0.0.255. If the IP address of a user is 192.168.8.1/24 and the IP address and mask specified by using this feature is 1.1.1.11/255.255.255.0, the source IP address of ARP detection packets is 192.168.8.11/24.

## Restrictions and guidelines

This feature takes effect only on users that come online after this feature is configured.

## Procedure

1. Enter system view.

**system-view**

2. Specify an IP address and mask for calculating the source IP of ARP detection packets.

```
port-security packet-detect arp-source-ip factor ip-address { mask | mask-length }
```

By default, no IP address or mask is specified for calculating the source IP of ARP detection packets. The source IP of ARP detection packets is 0.0.0.0.

## Command reference

### port-security packet-detect arp-source-ip factor

Use **port-security packet-detect arp-source-ip factor** to specify an IP address and mask for calculating the source IP of ARP detection packets.

Use **undo port-security packet-detect arp-source-ip factor** to restore the default.

## Syntax

```
port-security packet-detect arp-source-ip factor ip-address { mask | mask-length }
```

```
undo port-security packet-detect arp-source-ip factor
```

## Default

No IP address or mask is specified for calculating the source IP of ARP detection packets. The source IP of ARP detection packets is 0.0.0.0.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*ip-address* { *mask* | *mask-length* }: Specifies an IP address and mask for calculating the source IP of ARP detection packets. The *mask* argument represents the IP address mask, in dotted decimal notation. The mask cannot be 255.255.255.255. The *mask-length* argument represents the IP address mask length, in the range of 0 to 31.

## Usage guidelines

By default, the device uses 0.0.0.0 as the source IP address of ARP detection packets. The network might have users that cannot respond to ARP detection packets with source IP address 0.0.0.0. As a

result, the device inadequately determines that these users have gone offline. To resolve the issue, use this command to specify an IP address and mask for calculating the source IP of ARP detection packets sent to a user in conjunction with the user's IP address.

The device uses the following formula to calculate the source IP address of ARP detection packets: source IP = (user IP & specified mask) | (specified IP & ~specified mask). The ~mask parameter represents the reverse of a mask. For example, the reverse mask of 255.255.255.0 is 0.0.0.255. If the IP address of a user is 192.168.8.1/24 and the IP address and mask specified by using this command is 1.1.1.11/255.255.255.0, the source IP address of ARP detection packets is 192.168.8.11/24.

To avoid the source IP address of ARP detection packets being the same as the destination IP address, follow these restrictions and guidelines:

- The mask length specified by using this command must be equal to or longer than the mask length of users' IP addresses.
- The mask cannot be 255.255.255.255.

This command takes effect only on users that come online after this command is executed.

## Examples

# Specify 0.0.0.11/24 for calculating the source IP of ARP detection packets.

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

```
[Sysname] port-security packet-detect arp-source-ip factor 0.0.0.11 24
```

## Related commands

```
mac-authentication packet-detect retry
```

```
dot1x packet-detect retry
```

# New feature: Associating PoE with Track

## Associating PoE with Track

### About this task

The PoE module can collaborate with the Track module to monitor the link status between the device and a PD. For example, if the PD supports the NQA ICMP echo test, you can specify a track entry associated with NQA to test the reachability of the PD. The NQA ICMP echo test must be configured on a Layer 3 interface. The PI is a Layer 2 interface. You are required to create a VLAN interface for the ICMP echo test and assign the PI to the VLAN.

The Track module notifies the PoE module of the following monitoring results:

- **Positive**—The monitored object is reachable.
- **Negative**—The monitored object is unreachable.
- **NotReady**—The monitoring result is not ready because of reasons such as nonexistence of the NQA group associated with the track entry.

When the Track module detects failure of the link, it changes the track entry state from positive to negative, which triggers the PoE module to take the following actions:

- **alarm-only**: Outputs an SNMP notification and log.
- **alarm-reboot-pd**: Outputs an SNMP notification and log and reboots the PD connected to the PI.

For information about SNMP notifications, see SNMP configuration in *Network Management and Monitoring Configuration Guide*.

For information about logs, see information center configuration in *Network Management and Monitoring Configuration Guide*.

For information about the Track module, see track configuration in *High Availability Configuration Guide*.

## Procedure

1. Enter system view.  
**system-view**
  2. Enter PI view.  
**interface** *interface-type* *interface-number*
  3. Associate the PI with a track entry.  
**poe track** *track-entry-number* **action** { **alarm** | **alarm-reboot-pd** }
- By default, a PI is not associated with a track entry.

## Command reference

### poe track

Use **poe track** to associate a PI to a track entry.

Use **undo poe track** to restore the default.

### Syntax

```
poe track track-entry-number action { alarm | alarm-reboot-pd }  
undo poe track
```

### Default

A PI is not associated with any track entry.

### Views

PI view

### Predefined user roles

network-admin

### Parameters

**track-entry-number**: Specify a track entry ID in the range of 1 to 1024.

**action**: Specifies the action to be taken when the track entry state changes from positive to negative.

**alarm**: Outputs an SNMP notification and log.

**alarm-reboot-pd**: Outputs an SNMP notification and log and reboots the PD connected to the PI.

### Usage guidelines

This command uses a track entry to monitor the link status between the device and a PD and triggers the specified action when the track entry state changes from positive to negative. For more information about Track, see Track configuration in *High Availability Configuration Guide*.

If you configure this command multiple times in PI view, the most recent configuration takes effect.

## Examples

# Associate GigabitEthernet 1/0/1 with track entry 1 and enable the system to output an SNMP notification and log when the track entry state changes from positive to negative.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] poe track 1 action alarm
```

## New feature: many-to-one VLAN mapping

### Configuring many-to-one VLAN mapping

#### About many-to-one VLAN mapping

Configure many-to-one VLAN mapping to transmit the same type of traffic from different users in one VLAN.

#### About many-to-one VLAN mapping

- To ensure correct traffic forwarding from the service provider network to the customer network, do not configure many-to-one VLAN mapping together with the following features:
  - Disabling MAC address learning.
  - Setting the MAC learning limit.For more information about MAC address learning, see "Configuring the MAC address table."
- To avoid network connection failure in a many-to-one VLAN mapping environment, make sure that an ARP request has been sent from the customer-side port for the connection to the network-side port.

#### Many-to-one VLAN mapping tasks at a glance

1. [Configuring the customer-side port](#)
2. [Configuring the network-side port](#)

#### Configuring the customer-side port

1. Enter system view.  
**system-view**
2. Enter interface view.
  - Enter Layer 2 Ethernet interface view.  
**interface** *interface-type interface-number*
  - Enter Layer 2 aggregate interface view.  
**interface bridge-aggregation** *interface-number*
3. Set the link type of the port.  
**port link-type { hybrid | trunk }**  
By default, the link type of a port is **access**.
4. Assign the port to the original VLANs.
  - Assign the trunk port to the original VLANs  
**port trunk permit vlan** *vlan-id-list*  
By default, a trunk port is assigned to VLAN 1.
  - Assign the hybrid port to the original VLANs as a tagged member.

```
port hybrid vlan vlan-id-list tagged
```

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.

5. Configure a many-to-one VLAN mapping.

```
vlan mapping uni { range vlan-range-list | single vlan-id-list }  
translated-vlan vlan-id
```

By default, no VLAN mapping is configured on an interface.

## Configuring the network-side port

1. Enter system view.

```
system-view
```

2. Enter interface view.

- o Enter Layer 2 Ethernet interface view.

```
interface interface-type interface-number
```

- o Enter Layer 2 aggregate interface view.

```
interface bridge-aggregation interface-number
```

3. Set the link type of the port.

```
port link-type { hybrid | trunk }
```

By default, the link type of a port is **access**.

4. Assign the port to the translated VLAN.

- o Assign the trunk port to the translated VLAN.

```
port trunk permit vlan vlan-id-list
```

By default, a trunk port is assigned to VLAN 1.

- o Assign the hybrid port to the translated VLAN as a tagged member.

```
port hybrid vlan vlan-id-list tagged
```

By default, a hybrid port is an untagged member of the VLAN to which the port belongs when its link type is access.

## Command reference

### vlan mapping uni

Use **vlan mapping uni** to configure many-to-one VLAN mapping on an interface.

Use **undo vlan mapping uni** to cancel the many-to-one VLAN mapping configuration.

#### Syntax

```
vlan mapping uni { range vlan-range-list | single vlan-id-list }  
translated-vlan vlan-id
```

```
undo vlan mapping uni { range vlan-range-list | single vlan-id-list }  
translated-vlan vlan-id
```

#### Default

No many-to-one VLAN mapping is configured on an interface.

#### Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**uni range** *vlan-range-list* **translated-vlan** *vlan-id*: Specifies the original VLAN ranges and the translated VLAN for a many-to-one VLAN mapping on the customer-side port. The *vlan-range-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id1* to *vlan-id2*. The value range for VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument. The value range for the *vlan-id* argument is 1 to 4094. Different VLAN ranges cannot overlap. Any of the original VLANs cannot be the same as the translated VLAN.

**uni single** *vlan-id-list* **translated-vlan** *vlan-id*: Specifies the original VLANs and the translated VLAN for a many-to-one VLAN mapping on the customer-side port. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN IDs, each of which is in the range of 1 to 4094. The value range for the *vlan-id* argument is 1 to 4094. Any of the original VLANs cannot be the same as the translated VLAN.

## Examples

# Configure many-to-one VLAN mappings on the customer-side port to map VLANs 1 through 50 and VLAN 80 to VLAN 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] vlan mapping uni range 1 to 50 translated-vlan 101
[Sysname-GigabitEthernet1/0/2] vlan mapping uni single 80 translated-vlan 101
```

# New feature: Disabling receiving a specific type of ICMP messages

## Disabling receiving a specific type of ICMP messages

### About this task

By default, the device receives all types of ICMP messages. Such a setting might affect device performance if a large number of ICMP responses are received within a short time. To solve this issue, you can perform this task to disable the device from receiving a specific type of ICMP messages.

### Restrictions and guidelines

Disabling receiving ICMP messages of a specific type might affect network operation. Please use this feature with caution.

### Procedure

1. Enter system view.  
**system-view**
2. Disable the device from receiving a specific type of ICMP messages.  
**undo ip icmp { name icmp-name | type icmp-type code icmp-code } receive enable**

By default, the device receives all types of ICMP messages.

# Command reference

## ip icmp receive enable

Use **ip icmp receive enable** to enable the device to receive a specific type of ICMP messages.

Use **undo ip icmp receive enable** to disable the device from receiving a specific type of ICMP messages.

### Syntax

```
ip icmp { name icmp-name | type icmp-type code icmp-code } receive enable
undo ip icmp { name icmp-name | type icmp-type code icmp-code } receive enable
```

### Default

The device can receive all types of ICMP messages.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**name** *icmp-name*: Specifies an ICMP message name, a case-insensitive string of 1 to 20 characters.

**type** *icmp-type*: Specifies an ICMP message type. The value range for the *icmp-type* argument is 0 to 255.

**code** *icmp-code*: Specifies an ICMP message code. The value range for the *icmp-code* argument is 0 to 255.

### Usage guidelines



#### CAUTION:

Disabling receiving ICMP messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device receives all types of ICMP messages. Such a setting might affect device performance if a large number of ICMP responses are received within a short time. To solve this issue, you can perform this task to disable the device from receiving a specific type of ICMP messages.

[Table 1](#) shows common ICMP messages and the information they carry.

**Table 1 Common ICMP messages**

| Name               | Type | Code | Description                                                       |
|--------------------|------|------|-------------------------------------------------------------------|
| echo               | 8    | 0    | Echo request used to ping a target node.                          |
| echo-reply         | 0    | 0    | Echo reply sent by a target node after receiving an echo request. |
| fragmentneed-dfset | 3    | 4    | Packets that need fragmentation but have the DF bit set.          |
| host-redirect      | 5    | 1    | Host redirection.                                                 |
| host-tos-redirect  | 5    | 3    | Host ToS redirection.                                             |

| Name                 | Type | Code | Description                  |
|----------------------|------|------|------------------------------|
| host-unreachable     | 3    | 1    | Unreachable host.            |
| information-reply    | 16   | 0    | Information reply.           |
| information-request  | 15   | 0    | Information request.         |
| net-redirect         | 5    | 0    | Network redirection.         |
| net-tos-redirect     | 5    | 2    | Network ToS redirection.     |
| net-unreachable      | 3    | 0    | Unreachable network.         |
| parameter-problem    | 12   | 0    | Invalid parameter.           |
| port-unreachable     | 3    | 3    | Unreachable port.            |
| protocol-unreachable | 3    | 2    | Unreachable protocol.        |
| reassembly-timeout   | 11   | 1    | Fragment reassembly timeout. |
| source-quench        | 4    | 0    | Source quench message.       |
| source-route-failed  | 3    | 5    | Source route failure.        |
| timestamp-reply      | 14   | 0    | Timestamp reply.             |
| timestamp-request    | 13   | 0    | Timestamp request.           |
| ttl-exceeded         | 11   | 0    | TTL exceeded in transit.     |

## Examples

# Enable the device to receive ICMP echo reply messages.

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

```
[Sysname] ip icmp name echo-reply receive enable
```

# New feature: Disabling sending a specific type of ICMP messages

## Disabling sending a specific type of ICMP messages

### About this task

By default, the device sends all types of ICMP messages except the Destination Unreachable, Time Exceeded, and Redirect types. Attackers might obtain information from specific types of ICMP messages, causing security issues.

For security purposes, you can perform this task to disable sending ICMP messages of specific types.

### Restrictions and guidelines

Disabling sending ICMP messages of a specific type might affect network operation. Please use this feature with caution.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following operations:

- Execute the **ip icmp send enable** command.
- Execute one command as needed:
  - **ip unreachable enable**
  - **ip ttl-expires enable**



- o **ip redirects enable**

## Procedure

1. Enter system view.  
**system-view**
2. Disable the device from sending a specific type of ICMP messages.  
**undo ip icmp { name icmp-name | type icmp-type code icmp-code } send enable**  
By default, the device sends all types of ICMP messages except the Destination Unreachable, Time Exceeded, and Redirect types.

## Command reference

### ip icmp send enable

Use **ip icmp send enable** to enable the device to send a specific type of ICMP messages.

Use **undo ip icmp send enable** to disable the device from sending a specific type of ICMP messages.

### Syntax

```
ip icmp { name icmp-name | type icmp-type code icmp-code } send enable
undo ip icmp { name icmp-name | type icmp-type code icmp-code } send enable
```

### Default

The device can send all types of ICMP messages except the following ICMP messages:

- Destination Unreachable.
- Time Exceeded.
- Redirect.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**name** *icmp-name*: Specifies an ICMP message name, a case-insensitive string of 1 to 20 characters.

**type** *icmp-type*: Specifies an ICMP message type. The value range for the *icmp-type* argument is 0 to 255.

**code** *icmp-code*: Specifies an ICMP message code. The value range for the *icmp-code* argument is 0 to 255.

### Usage guidelines



#### CAUTION:

Disabling sending ICMP messages of a specific type might affect network operation. Please use this feature with caution.

By default, the device sends all types of ICMP messages except the Destination Unreachable, Time Exceeded, and Redirect types. Attackers might obtain information from specific types of ICMP messages, causing security issues.

For security purposes, you can use this command to disable the device from sending ICMP messages of specific types.

To enable sending Destination Unreachable, Time Exceeded, or Redirect messages, you can perform one of the following operations:

- Execute the **ip icmp send enable** command.
- Execute one command as needed:
  - **ip unreachable enable**
  - **ip ttl-expires enable**
  - **ip redirects enable**

Table 2 shows common ICMP messages and the information they carry.

**Table 2 Common ICMP messages**

| Name                 | Type | Code | Description                                                       |
|----------------------|------|------|-------------------------------------------------------------------|
| echo                 | 8    | 0    | Echo request used to ping a target node.                          |
| echo-reply           | 0    | 0    | Echo reply sent by a target node after receiving an echo request. |
| fragmentneed-dfset   | 3    | 4    | Packets that need fragmentation but have the DF bit set.          |
| host-redirect        | 5    | 1    | Host redirection.                                                 |
| host-tos-redirect    | 5    | 3    | Host ToS redirection.                                             |
| host-unreachable     | 3    | 1    | Unreachable host.                                                 |
| information-reply    | 16   | 0    | Information reply.                                                |
| information-request  | 15   | 0    | Information request.                                              |
| net-redirect         | 5    | 0    | Network redirection.                                              |
| net-tos-redirect     | 5    | 2    | Network ToS redirection.                                          |
| net-unreachable      | 3    | 0    | Unreachable network.                                              |
| parameter-problem    | 12   | 0    | Invalid parameter.                                                |
| port-unreachable     | 3    | 3    | Unreachable port.                                                 |
| protocol-unreachable | 3    | 2    | Unreachable protocol.                                             |
| reassembly-timeout   | 11   | 1    | Fragment reassembly timeout.                                      |
| source-quench        | 4    | 0    | Source quench message.                                            |
| source-route-failed  | 3    | 5    | Source route failure.                                             |
| timestamp-reply      | 14   | 0    | Timestamp reply.                                                  |
| timestamp-request    | 13   | 0    | Timestamp request.                                                |
| ttl-exceeded         | 11   | 0    | TTL exceeded in transit.                                          |

## Examples

# Enable the device to send ICMP echo reply messages.

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

```
[Sysname] ip icmp name echo-reply send enable
```

# New feature: MAC swap loopback test configuration

## Configuring a MAC swap loopback test

### About this task

A MAC swap loopback test is an interruptive performance test. The following MAC swap loopback tests are available based on the usage scenario:

- **Local MAC swap loopback test**—Checks connectivity and performance of the network between a tester and a tested switch, and performance of the tested switch. After Ethernet frames sent by a tester reach a downlink interface of a switch on which the local MAC swap loopback test is configured, the downlink interface swaps source and destination MAC addresses of the Ethernet frames. Then, the switch sends the Ethernet frames back to the tester through a specified interface for the tester to obtain information about the network connectivity and performance.
- **Remote MAC swap loopback test**—Checks connectivity and performance of the network between a tester and a tested switch without checking performance of the tested switch. After Ethernet frames sent by a tester reach an uplink interface of a switch on which the remote MAC swap loopback test is configured, the uplink interface swaps source and destination MAC addresses of the Ethernet frames. Then, the switch sends the Ethernet frames back to the tester through the uplink interface for the tester to obtain information about the uplink network connectivity and performance.

### Restrictions and guidelines

The MAC swap loopback test feature interrupts all services of a tested interface. Make sure you are fully aware of the impacts of this feature when you configure it on a live network.

### Procedure

1. Enter Ethernet interface view.  
`interface interface-type interface-number`
2. Configure MAC swap loopback tests.
  - Configure the local MAC swap loopback test.  
`loopback local swap-mac source-mac source-mac-address dest-mac dest-mac-address vlan vlan-id [ inner-vlan inner-vlan-id ]  
interface interface-type interface-number [ timeout { time-value | none } ]`  
By default, the local MAC swap loopback test is disabled on an interface.
  - Configure the remote MAC swap loopback test.  
`loopback remote swap-mac source-mac source-mac-address dest-mac dest-mac-address vlan vlan-id [ inner-vlan inner-vlan-id ]  
[ timeout { time-value | none } ]`  
By default, the remote MAC swap loopback test is disabled on an interface.
3. Start MAC swap loopback tests.  
`loopback swap-mac start`  
By default, MAC swap loopback tests are stopped on an interface.

## Command reference

### loopback local swap-mac

Use `loopback local swap-mac` to enable the local MAC swap loopback test.

Use `undo loopback local swap-mac` to disable the local MAC swap loopback test.

## Syntax

```
loopback local swap-mac source-mac source-mac-address dest-mac
dest-mac-address vlan vlan-id [ inner-vlan inner-vlan-id ] interface
interface-type interface-number [ timeout { time-value | none } ]

undo loopback local swap-mac
```

## Default

The local MAC swap loopback test is disabled on an interface.

## Views

Ethernet interface view

## Predefined user roles

network-admin  
network-operator

## Parameters

**source-mac-address:** Specifies a source MAC address. The source MAC address must be a unicast MAC address.

**dest-mac-address:** Specifies a destination MAC address. The destination MAC address must be a unicast MAC address.

**vlan-id:** Specifies a VLAN ID in the range of 1 to 4094.

**inner-vlan-id:** Specifies an inner VLAN ID in the range of 1 to 4094.

**time-value:** Sets the loopback test timeout timer in the range of 5 to 300 seconds. The default value is 60. When the timer expires, the system automatically stops MAC swap loopback tests.

**none:** Disables the loopback test timeout timer. MAC swap loopback tests can only be disabled manually.

## Usage guidelines

The local MAC swap loopback test checks connectivity and performance of the network between a tester and a tested switch, and performance of the tested switch.

After Ethernet frames sent by a tester reach a downlink interface of a switch on which the local MAC swap loopback test is configured, the downlink interface swaps source and destination MAC addresses of the Ethernet frames. Then, the switch sends the Ethernet frames back to the tester through the downlink interface for the tester to obtain information about the network connectivity and performance.

## Examples

# Configure the local MAC swap loopback test.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback local swap-mac source-mac 00e0-fc00-0085
dest-mac 00e0-fc00-1004 vlan 100 interface gigabitethernet 1/0/2
```

## Related commands

```
loopback remote swap-mac
loopback swap-mac
display loopback swap-mac information
```

## loopback remote swap-mac

Use **loopback remote swap-mac** to enable the remote MAC swap loopback test.

Use **undo loopback remote swap-mac** to disable the remote MAC swap loopback test.

### Syntax

```
loopback remote swap-mac source-mac source-mac-address dest-mac
dest-mac-address vlan vlan-id [ inner-vlan inner-vlan-id ] [ timeout
{ time-value | none } ]
undo loopback remote swap-mac
```

### Default

The remote MAC swap loopback test is disabled on an interface.

### Views

Ethernet interface view

### Predefined user roles

network-admin  
network-operator

### Parameters

**source-mac-address**: Specifies a source MAC address. The source MAC address must be a unicast MAC address.

**dest-mac-address**: Specifies a destination MAC address. The destination MAC address must be a unicast MAC address.

**vlan-id**: Specifies a VLAN ID in the range of 1 to 4094.

**inner-vlan-id**: Specifies an inner VLAN ID in the range of 1 to 4094.

**time-value**: Sets the loopback test timeout timer in the range of 5 to 300 seconds. The default value is 60. When the timer expires, the system automatically stops MAC swap loopback tests.

**none**: Disables the loopback test timeout timer. MAC swap loopback tests can only be disabled manually.

### Usage guidelines

The remote MAC swap loopback test checks connectivity and performance of the network between a tester and a tested switch without checking performance of the tested switch.

After Ethernet frames sent by a tester reach an uplink interface of a switch on which the remote MAC swap loopback test is configured, the uplink interface swaps source and destination MAC addresses of the Ethernet frames. Then, the switch sends the Ethernet frames back to the tester through the uplink interface for the tester to obtain information about the uplink network connectivity and performance.

### Examples

# Configure the remote MAC swap loopback test.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback local swap-mac source-mac 00e0-fc00-0085
dest-mac 00e0-fc00-1004 vlan 100
```

### Related commands

**loopback local swap-mac**

```
loopback swap-mac
display loopback swap-mac information
```

## loopback swap-mac

Use **loopback swap-mac** to start or stop MAC swap loopback tests.

### Syntax

```
loopback swap-mac [ start | stop ]
```

### Default

MAC swap loopback tests are stopped on an interface.

### Views

Ethernet interface view

### Predefined user roles

network-admin  
network-operator

### Parameters

**start**: Starts MAC swap loopback tests.  
**stop**: Stops MAC swap loopback tests.

### Usage guidelines

Both the remote and local MAC swap loopback tests affect operation of the network. To minimize the impact of the loopback tests on the network, plan the testing window according to your services and perform the loopback tests within the testing window.

MAC swap loopback tests can be stopped manually or automatically upon expiration of the loopback test timeout timer. To start the loopback tests again, execute the **loopback swap-mac start** command.

### Examples

```
# Start MAC swap loopback tests.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback swap-mac start
```

### Related commands

```
loopback local swap-mac
loopback remote swap-mac
display loopback swap-mac information
```

## display loopback swap-mac information

Use **display loopback swap-mac information** to display configuration of MAC swap loopback tests.

### Syntax

```
display loopback swap-mac information
```

### Views

Any view

## Predefined user roles

network-admin  
network-operator

## Examples

# Display configuration of the local MAC swap loopback test.

```
<Sysname> display loopback swap-mac information
  Loopback type           : local
  Loopback state          : running
  Loopback test times(s)  : 60
  Loopback interface      : GigabitEthernet1/0/1
  Loopback output interface : GigabitEthernet1/0/2
  Loopback source MAC     : 0001-0001-0001
  Loopback destination MAC : 0002-0002-0002
  Loopback vlan           : 10
  Loopback inner vlan     : 0
  Loopback packets        : 0
  Drop packets            : 3
```

# Display configuration of the remote MAC swap loopback test.

```
<Sysname> display loopback swap-mac information
  Loopback type           : remote
  Loopback state          : running
  Loopback test time(s)   : 60
  Loopback interface      : GigabitEthernet1/0/1
  Loopback source MAC     : 0001-0001-0001
  Loopback destination MAC : 0002-0002-0002
  Loopback vlan           : 10
  Loopback inner vlan     : 0
  Loopback packets        : 0
  Drop packets            : 3
```

**Table 3 Command output**

| Field                     | Description                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loopback type             | Type of the MAC swap loopback test: <ul style="list-style-type: none"><li>• <b>Local.</b></li><li>• <b>Remote.</b></li></ul>                                                   |
| Loopback state            | State of the loopback test: <ul style="list-style-type: none"><li>• <b>Running</b>—The loopback test is running.</li><li>• <b>Stop</b>—The loopback test is stopped.</li></ul> |
| Loopback test time(s)     | Value of the loopback test timeout timer. This field displays <b>None</b> if the timeout timer is disabled.                                                                    |
| Loopback interface        | Interface under loopback test.                                                                                                                                                 |
| Loopback output interface | Interface sending backup loopback testing frames.                                                                                                                              |
| Loopback source MAC       | Source MAC address in the loopback testing frames.                                                                                                                             |
| Loopback destination MAC  | Destination MAC address in the loopback testing frames.                                                                                                                        |
| Loopback vlan             | VLAN ID of the loopback testing frames.                                                                                                                                        |

|                     |                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Loopback inner vlan | Inner VLAN ID of the loopback testing frames.                                                                                                      |
| Loopback packets    | Number of received loopback testing frames.                                                                                                        |
| Drop packets        | Number of discarded loopback testing packets that do not meet the requirements. This field is displayed only for the local MAC swap loopback test. |

### Related commands

```

loopback local swap-mac
loopback remote swap-mac
loopback swap-mac

```

## New feature: Configuring the TMPDO for the MPS

### Configuring the TMPDO for the MPS

#### About this task

The Maintain Power Signature (MPS) is an electrical signature provided by a PD. The PD uses this signature to maintain connection to the PSE in sleep mode. The PD sends a PoE-compliant pulse current to the PSE periodically. If the PSE detects the PoE-compliant pulse current from the PD within the TMPDO, it supplies power to the PD. If the PSE does not detect the PoE-compliant pulse current from the PD within the TMPDO, it will not supply power to the PD.

To send pulse currents at larger intervals for lower standby power, you can use this command to change the TMPDO to be longer.

#### Restrictions and guidelines

Only PSE modules that have a model name of LSPPSE\*\*A support this feature. To view the PSE models, execute the **display poe pse** command.

If you execute the command multiple times, the most recent configuration takes effect.

#### Procedure

1. Enter System view.  
**system-view**
2. Set the TMPDO for the MPS.  
**poe mps pse *pse-id* tmpdo { *timer* | long | normal }**

By default, the normal TMPDO mode is used for the MPS. The TMPDO for the MPS is 324 milliseconds.

### Command reference

#### poe mps

Use **poe mps** to set the TMPDO for MPS.

Use **undo poe mps** to restore the default.

#### Syntax

```

poe mps pse pse-id tmpdo { timer | long | normal }
undo poe mps pse pse-id tmpdo

```



## Default

The normal TMPDO mode is used for the MPS. The TMPDO is 324 milliseconds.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*pse-id*: Specifies a PSE by its ID.

*timer*: Sets the TMPDO for the MPS. The value is a multiple of 4 in the range of 300 to 400, in milliseconds.

**long**: Specify the long TMPDO mode. The TMPDO is 360 milliseconds.

**normal**: Specifies the normal TMPDO mode. The TMPDO is 324 milliseconds.

## Usage guidelines

The MPS is an electrical signature provided by a PD. The PD uses this signature to maintain connection to the PSE in sleep mode. The PD sends a PoE-compliant pulse current to the PSE periodically. If the PSE detects the PoE-compliant pulse current from the PD within the TMPDO, it supplies power to the PD. If the PSE does not detect the PoE-compliant pulse current from the PD within the TMPDO, it will not supply power to the PD.

To send pulse currents at larger intervals for lower standby power, you can use this command to change the TMPDO to be longer.

Only PSE modules that have a model name of LSPPSE\*\*A support this feature. To view the PSE models, execute the **display poe pse** command.

If you execute the command multiple times, the most recent configuration takes effect.

## Examples

# Set the TMPDO for the MPS to 350 milliseconds.

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

```
[Sysname] poe mps pse 1 tmpdo 350
```

# New feature: Configuring port collaboration

## Configuring port collaboration

### Restrictions and guidelines

Port collaboration takes effect only on the ports with outward-facing MEPs configured.

### Procedure

1. Enter system view.  
**system-view**
2. Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.  
**interface** *interface-type* *interface-number*
3. Configure port collaboration.  
**cfg port-trigger { cc-expire | rdi } action { block | shutdown }**  
By default, port collaboration is not configured.

# Command reference

## cfp port-trigger

Use **cfp port-trigger** to specify the triggering event and triggered action for port collaboration.

Use **undo cfp port-trigger** to cancel the triggering event and triggered action for port collaboration.

### Syntax

```
cfp port-trigger { cc-expire | rdi } action { block | shutdown }
undo cfp port-trigger { cc-expire | rdi } action
cfp port-trigger remote-status action shutdown
undo cfp port-trigger remote-status action
```

### Default

The triggering event and triggered action are not specified for port collaboration.

### Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

### Predefined user roles

network-admin

### Parameters

**cc-expire**: Triggers port collaboration when continuity check expires.

**rdi**: Triggers port collaboration when the CCMs with the RDI flag bit set are received.

**remote-status**: Triggers port collaboration when the inward-facing MEP detects that the remote MEP interface is down.

**block**: Blocks the port by changing its link layer protocol state to DOWN (CFD). The port cannot send or receive any data packets.

**shutdown**: Shuts down the port by changing its physical state to CFD DOWN. The port cannot send or receive any data packets or protocol packets.

### Usage guidelines

After you execute this command, CFD blocks or shuts down the associated port upon detecting a link failure.

If a port is blocked by CFD, it can automatically come up when the link recovers.

If a port is shut down by CFD, it cannot automatically come up when the link recovers.

- If port collaboration is triggered by continuity check expiration, you must execute the **undo shutdown** or **undo cfp port-trigger { cc-expire | rdi } action** command to bring up the port.
- If port collaboration is triggered by CCMs with the RDI flag bits set, you must execute the **undo cfp port-trigger { cc-expire | rdi } action** command to bring up the port.
- If port collaboration is triggered by remote interface failure, you must execute the **undo cfp port-trigger remote-status action** command to bring up the port. In this triggering event, port collaboration shuts down only the inward-facing MEP interface in up state on the local end.

You can specify multiple triggering events for an interface. All the triggering events can take effect. When you specify multiple triggered actions for a triggering event on an interface, the most recent configuration takes effect.

The command takes effect only on the ports with outward-facing MEPs configured.

Configurations in Ethernet interface view take effect only on the current interface.

Configurations in aggregate interface view take effect only on the current aggregate interface.

If the MEP belongs to an MA that does not carry the VLAN attribute, configurations on a member port of an aggregation group take effect only on the current member port.

If the MEP belongs to an MA that carries the VLAN attribute, configurations on a member port of an aggregation group take effect only when the member port leaves the aggregation group.

## Examples

# Specify the triggering event as **cc-expire** and the triggered action as **block** for port collaboration on GigabitEthernet 1/0/1.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] cfd port-trigger cc-expire action block
```

# Specify the triggering event as **cc-expire** and the triggered action as **shutdown** for port collaboration on GigabitEthernet 1/0/1.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] cfd port-trigger cc-expire action shutdown
```

## Related commands

```
cfd cc enable
```

```
cfd mep
```

# New feature: Disabling PoE power supply on shutdown interfaces

## Disabling PoE power supply on shutdown interfaces

### About this task

By default, the device continues supplying power to an interface after the interface is shut down by the **shutdown** command or by an upper layer module such as monitor link. As a result, the PD connected to the shutdown interface operates continuously but fails to access the network.

This task disables the PoE module from supplying power to an interface after the interface is shut down. After the interface comes up, the PoE module resumes power supply to the interface.

### Restrictions and guidelines

The command does not power off an interface that has been shut down but is supplying power to a PD.

### Procedure

1. Enter system view.  
**system-view**
2. Disable PoE power supply on shutdown interfaces.  
**poe track-shutdown**

By default, the device continues supplying power to an interface after the interface is shut down.

## Command reference

### poe track-shutdown

Use **poe track-shutdown** to disable PoE power supply on shutdown interfaces.

Use **undo poe track-shutdown** to restore the default.

#### Syntax

**poe track-shutdown**

**undo poe track-shutdown**

#### Default

The device continues supplying power to an interface after the interface is shut down.

#### Views

System view

#### Predefined user roles

network-admin

#### Usage guidelines

By default, the device continues supplying power to an interface after the interface is shut down by the **shutdown** command or by an upper layer module such as monitor link. As a result, the PD connected to the shutdown interface operates continuously but fails to access the network.

This command disables the PoE module from supplying power to an interface after the interface is shut down. After the interface comes up, the PoE module resumes power supply to the interface.

The command does not power off an interface that has been shut down but is supplying power to a PD.

#### Examples

# Disable PoE power supply on interfaces after they shut down.

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

```
[Sysname] poe track-shutdown
```

#### Related commands

**poe enable**

## New feature: Configuring PoE delay

### Configuring PoE delay

#### About this task

By default, the device executes the **poe enable** command and supplies power to an interface immediately when any one of the following conditions is met:

- The **poe enable** command is configured.
- The device reboots with the **poe enable** command in the configuration file.
- The interface comes up and the PoE module resumes PoE power supply to the interface.

This task creates a PoE delay timer after the **poe enable** command is executed and allows the PoE module to supply power to the PI only after the timer expires.

## Restrictions and guidelines

The **undo poe enable** command is executed immediately upon configuration and is not affected by this task.

## Procedure

1. Enter system view.  
**system-view**
2. Enable PoE delay.  
**poe power-delay** *time*  
By default, PoE delay is disabled.

## Command reference

### poe power-delay

Use **poe power-delay** to enable PoE delay.

Use **undo poe power-delay** to disable PoE delay.

### Syntax

```
poe power-delay time  
undo poe power-delay
```

### Default

PoE delay is disabled.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*time*: Specifies the delay time in the range of 1 to 3600, in seconds.

## Usage guidelines

By default, the device executes the **poe enable** command and supplies power to an interface immediately when any one of the following conditions is met:

- The **poe enable** command is configured.
- The device reboots with the **poe enable** command in the configuration file.
- The interface comes up and the PoE module resumes PoE power supply to the interface.

The **poe power-delay** creates a PoE delay timer after the **poe enable** command is executed and allows the PoE module to supply power to the PI only after the timer expires.

The **undo poe enable** command is executed immediately upon configuration and is not affected by the **poe power-delay** command.

## Examples

```
# Enable PoE delay and set the delay time to 30 seconds.  
<Sysname> system-view
```

```
[Sysname] poe power-delay 30
```

## Related commands

```
poe enable
```

# New feature: Setting the PoE guard band

## Setting the PoE guard band

### About this task

PoE guard band is a specified amount of power reserved to prevent PSE power overload in case of PD power jitter. For example, if the maximum power of the PSE is 200 W and the guard band is 30 W, the PSE can provide a maximum power of 170 W to all PDs. If the total power of PDs reaches 170 W, no power will be supplied to new PDs.

When the PD operates stably with low power jitter (less than the default guard band), you can use the **poe pse guard-band** command to decrease the guard band and use the released PSE power to power the new PDs.

### Procedure

1. Enter system view.  
**system-view**
2. Set the PoE guard band.  
**poe pse *pse-id* guard-band *power***  
**undo poe pse *pse-id* guard-band *power***  
By default, the PoE guard band is 30 W.

## Command reference

### poe guard-band

Use **poe guard-band** to set the PoE guard band.

Use **undo poe guard-band** to restore the default.

### Syntax

```
poe pse pse-id guard-band power  
undo poe pse pse-id guard-band power
```

### Default

By default, the PoE guard band is 30 W.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*pse-id*: Specifies a PSE by its ID.

*power*: Specifies the PoE guard band in the range of 0 to 30, in watts.

## Usage guidelines

### Application scenarios

PoE guard band is a specified amount of power reserved to prevent PSE power overload in case of PD power jitter. For example, if the maximum power of the PSE is 200 W and the guard band is 30 W, the PSE can provide a maximum power of 170 W to all PDs. If the total power of PDs reaches 170 W, no power will be supplied to new PDs.

When the PD operates stably with low power jitter (less than the default guard band), you can use the **poe pse guard-band** command to reduce the guard band and use the released PSE power to power the new PDs.

### Restrictions and guidelines

Before executing this command, execute the **display poe interface** command to check the value of the **Remaining** field. If the guard band is greater than the value of **Remaining** field, some PDs being powered might have a power down. For example, the current guard band is 10 W, and the value of the **Remaining** field is 10 W. If the network administrator changes the guard band to 30 W, some PDs that are currently being powered might have a power down to make up for the 20 W power gap.

## Examples

```
# Set the PoE guard band to 30 W.  
<Sysname> system-view  
[Sysname] poe pse-id 1 guard-band 30
```

# New feature: Configuring a PD disconnection detection mode

## Configuring a PD disconnection detection mode

### CAUTION:

If you change the PD disconnection detection mode when the device is running, the connected PDs are powered off. Be aware of the impact of this operation before you perform it.

### About this task

A PSE detects PD disconnection in AC mode or DC mode. The AC mode uses less power than the DC mode.

### Procedure

1. Enter system view.  
**system-view**
2. Configure a PD disconnection detection mode.  
**poe disconnect { ac | dc }**  
The default PD disconnection detection mode is AC.

## Command reference

### poe disconnect

Use **poe disconnect** to configure a PD disconnection detection mode.

Use `undo poe disconnect` to restore the default.

## Syntax

```
poe disconnect { ac | dc }  
undo poe disconnect
```

## Default

The default PD disconnection detection mode is AC.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**ac**: Specifies the PD disconnection detection mode as **ac**.

**dc**: Specifies the PD disconnection detection mode as **dc**.

## Usage guidelines

If you change the PD disconnection detection mode while the device is running, the connected PDs are powered off.

## Examples

```
# Set the PD disconnection detection mode to dc.
```

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

```
[Sysname] poe disconnect dc
```

## Related commands

```
display poe pse
```

# New feature: Ignoring the PD power class

## Ignoring the PD power class

### About this task

Before supplying power to a PD, the device detects the power class of the PD by default. For example, if the device detects the power class of a PD as 1, the device can provide a maximum power of 12.95 W to the PD. If the power required by a PD is greater than 12.95 W, the device will stop supplying power to the PD.

### Restrictions and guidelines

After configuring this task, the device will continue to detect the PD power class before supplying power to a PD. As long as the power required by the PD does not exceed the maximum power on the interface (configured by using the `poe max power` command in interface view), the device can supply power to the PD.

If you execute the `poe class-detect ignore` command multiple times, and the most recent configuration will take effect.

## Procedure

1. Enter system view.

```
system-view
```



2. Enter PI view.

```
interface interface-type interface-number
```

3. Ignore the PD power class.

```
poe class-detect ignore
```

By default, the device supplies power to PDs based on the detected PD power class.

## Command reference

### poe class-detect ignore

Use `poe class-detect ignore` to ignore the PD power class.

Use `undo poe class-detect` to restore the default.

#### Syntax

```
poe class-detect ignore
undo poe class-detect
```

#### Default

The device supplies power to a PD based on the detected power class of the PD.

#### Views

PI view

#### Predefined user roles

network-admin

#### Usage guidelines

Before supplying power to a PD, the device detects the power class of the PD by default. For example, if the device detects the power class of 1 for a PD, the device can provide a maximum power of 12.95 W to the PD. If the power required by a PD is greater than 12.95 W, the device will stop supplying power to the PD.

After configuring this command, the device will continue to detect the PD power class before supplying power to a PD. As long as the power required by the PD does not exceed the maximum power on the interface (configured by using the `poe max power` command in interface view), the device can supply power to the PD.

If you execute the `poe class-detect ignore` command multiple times, and the most recent configuration will take effect.

#### Examples

# Configure the GigabitEthernet1/0/1 to ignore the PD power class.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe class-detect ignore
```

## Modified feature: Applying a portal Web server to an interface

### Feature change description

As from this release, the device supports applying a secondary portal Web server to an interface.

## Command changes

Modified command: portal apply web-server

### Old syntax

```
portal [ ipv6 ] apply web-server server-name [ fail-permit ]
undo portal [ ipv6 ] apply web-server
```

### New syntax

```
portal [ ipv6 ] apply web-server server-name [ fail-permit | secondary ]
undo portal [ ipv6 ] apply web-server [ server-name ]
```

### Views

Interface view

### Change description

The **secondary** keyword was added to the command to support applying a secondary portal Web server to the interface.

## Modified feature: Displaying portal configuration and running information on an interface

### Feature change description

As from this release, the device supports displaying secondary portal Web server information on an interface.

## Command changes

Modified command: display portal

### Syntax

```
display portal interface interface-type interface-number
```

### Views

Any view

### Change description

Before modification: This command does not display information about secondary portal Web servers configured on interfaces.

After modification: This command can display information about secondary portal Web servers configured on interfaces, for example:

# Display portal configuration and running information on VLAN-interface 2.

```
<Sysname> display portal interface vlan-interface 2
```

```
Portal information of Vlan-interface2
```

```
NAS-ID profile: aaa
VSRP instance : instancel
VSRP status    : Master
Authorization   : Strict checking
```

```

ACL          : Enabled
User profile : Disabled
Dual stack   : Disabled
Max users    : Not configured
IPv4:
  Portal status: Enabled
  Portal authentication method: Direct
  Portal VSRP status: M_Delay
  Portal web server: wbs(active)
  Secondary portal Web server: wbsec
  Portal mac-trigger-server: mts
  Authentication domain: my-domain
  Pre-auth domain: abc
  User-dhcp-only: Enabled
  Pre-auth IP pool: ab
  Max users: Not configured
  Bas-ip: Not configured
  User detection: Type: ICMP Interval: 300s Attempts: 5 Idle time: 180s
  Action for server detection:
    Server type  Server name  Action
    Web server   wbs         fail-permit
    Portal server pts         fail-permit
  Layer3 source network:
    IP address      Mask
    1.1.1.1         255.255.0.0

  Destination authentication subnet:
    IP address      Mask
    2.2.2.2         255.255.255.0

IPv6:
  portal status: Disabled
  Portal authentication method: Disabled
  Portal VSRP status: M_Alone
  Portal web server: Not configured
  Secondary portal Web server: Not configured
  Portal mac-trigger-server: Not configured
  Authentication domain: Not configured
  Pre-auth domain: Not configured
  User-dhcp-only: Disabled
  Pre-auth IP pool: Not configured
  Max users: Not configured
  Bas-ipv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type  Server name  Action
    --          --          --
  Layer3 source network:

```

IP address

Prefix length

Destination authentication subnet:

IP address

Prefix length

## Modified feature: Display power supply information

### Feature change description

As from this release, if pluggable power supplies except PSR180-56A are installed on PoE models, the **display power** command displays the output current, voltage, and power information of the power supplies. The command output from the **display power** command is for reference only. The actual data is subject to professional testing.

### Command changes

#### Modified command: display power

##### Syntax

```
display power [ slot slot-number [ power-id ] ]
```

##### Views

Any view

##### Change description

Before modification: The **Current(A)**, **Voltage(V)**, and **Power(W)** fields in the command output are displayed two hyphens (--). The device does not support collection information about these fields.

After modification: If pluggable power supplies except PSR180-56A are installed on PoE models, the **display power** command displays the output current, voltage, and power information of the power supplies. The **Current(A)**, **Voltage(V)**, **Power(W)** fields in the command output are for reference only. The actual data is subject to professional testing.

##### Examples

# Display power supply information.

```
<Sysname> display power
```

| PowerID | State  | Mode | Current(A) | Voltage(V) | Power(W) |
|---------|--------|------|------------|------------|----------|
| 1       | Normal | AC   | 5.95       | 11.95      | 72       |
| 2       | Absent | --   | --         | --         | --       |

## Modified feature: Configuring the padding mode and padding format for the Circuit ID sub-option in VLAN view

### Feature change description

As from this release, you can configure the padding mode and padding format for the Circuit ID sub-option in VLAN view.

## Command changes

### Modified command: dhcp snooping information circuit-id

#### Syntax

```
dhcp snooping information circuit-id { normal-extended | [ vlan vlan-id ]  
string circuit-id | { normal | verbose [ node-identifier { mac | sysname |  
user-defined node-identifier } ] } [ format { ascii | hex } ] }  
undo dhcp snooping information circuit-id [ vlan vlan-id ]
```

#### Views

Layer 2 Ethernet interface view  
Layer 2 aggregate interface view  
VLAN view

#### Change description

Before modification: You cannot configure the padding mode and padding format for the Circuit ID sub-option in VLAN view.

After modification: You can configure the padding mode and padding format for the Circuit ID sub-option in VLAN view, but the `vlan vlan-id` option is not supported in VLAN view.

## Modified feature: Enabling DHCP snooping to support Option 82 in VLAN view

### Feature change description

As from this release, you can enable DHCP snooping to support Option 82 in VLAN view.

## Command changes

### Modified command: dhcp snooping information enable

#### Syntax

```
dhcp snooping information enable  
undo dhcp snooping information enable
```

#### Views

VLAN view

#### Change description

Before modification: You cannot enable DHCP snooping to support Option 82 in VLAN view.

After modification: You can enable DHCP snooping to support Option 82 in VLAN view.

## Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option in VLAN view

### Feature change description

As from this release, you can configure the padding mode and padding format for the Remote ID sub-option in VLAN view. To specify the hexadecimal padding format, you can specify the **hex** keyword.

### Command changes

Modified command: dhcp snooping information remote-id

#### Old syntax

```
dhcp snooping information remote-id { normal [ format ascii ] | { hex remote-id  
| string remote-id | sysname } }  
undo dhcp snooping information remote-id
```

#### New syntax

```
dhcp snooping information remote-id { normal [ format { ascii | hex } ]  
| { hex remote-id | string remote-id | sysname } }  
undo dhcp snooping information remote-id
```

#### Views

VLAN view

#### Change description

Before modification: In VLAN view, you cannot configure the padding mode and padding format for the Remote ID sub-option and the **hex** keyword is not supported.

After modification: In VLAN view, you can configure the padding mode and padding format for the Remote ID sub-option and the **hex** keyword is supported. To specify the hexadecimal padding format, you can specify the **hex** keyword.

## Modified feature: Configuring the Option 82 handling strategy for DHCP request messages in VLAN view

### Feature change description

As from this release, you can configure the Option 82 handling strategy for DHCP request messages in VLAN view.

## Command changes

### Modified command: dhcp snooping information strategy

#### Syntax

```
dhcp snooping information strategy { append | drop | keep | replace }  
undo dhcp snooping information strategy
```

#### Views

VLAN view

#### Change description

Before modification: You cannot configure the Option 82 handling strategy for DHCP request messages in VLAN view.

After modification: You can configure the Option 82 handling strategy for DHCP request messages in VLAN view.

## Modified feature: Configuring the padding mode for the Vendor-Specific sub-option in VLAN view

### Feature change description

As from this release, you can configure the padding mode for the Vendor-Specific sub-option in VLAN view.

## Command changes

### Modified command: dhcp snooping information vendor-specific

#### syntax

```
dhcp snooping information vendor-specific bas [ node-identifier { mac |  
sysname | user-defined string } ]  
undo dhcp snooping information vendor-specific
```

#### Views

VLAN view

#### Change description

Before modification: You cannot configure the padding mode for the Vendor-Specific sub-option in VLAN view.

After modification: You can configure the padding mode for the Vendor-Specific sub-option in VLAN view.

## Modified feature: Changing the default settings for outputting port state transition information

### Feature change description

As from this release, If the device starts up the factory defaults, outputting port state transition information is enabled.

### Command changes

Modified command: `stp port-log`

#### Syntax

```
stp port-log { all | instance instance-list | vlan vlan-id-list }  
undo stp port-log { all | instance instance-list | vlan vlan-id-list }
```

#### Views

System view

#### Change description

Before modification: By default, if the device starts up the factory defaults, outputting port state transition information is disabled.

After modification: By default, if the device starts up the factory defaults, outputting port state transition information is enabled.

## Modified feature: Support of 10G fiber ports for 2.5G transceiver modules

### Feature change description

As from this version, 10G fiber ports support 2.5G transceiver modules. You can use the **speed 2500** command to configure a port to operate at 2500 Mbps.

### Command changes

Modified command: `speed`

#### Old syntax

```
speed { 1000 | 10000 | auto }
```

#### New syntax

```
speed { 1000 | 2500 | 10000 | auto }
```

#### Views

10G interface view

#### Change description

Before modification: The **2500** keyword is not supported.



After modification: The **2500** keyword is supported.

**2500**: Sets the speed to 2500 Mbps.

## Modified feature: PD detection mode

### Feature change description

As from this version, if the device starts up with factory default settings, it supplies power to PDs that comply with basic requirements of 802.3af or 802.3at.

### Command changes

Modified command: `poe detection-mode`

#### Syntax

```
poe detection-mode { none | simple | strict }
```

#### Views

PI view

#### Change description

Before modification: By default, the device supplies power to PDs that comply with all requirements of 802.3af or 802.3at if it starts up with factory default settings.

After modification: By default, the device supplies power to PDs that comply with basic requirements of 802.3af or 802.3at if it starts up with factory default settings.

**none**: Enables the device to supply power to PDs that are correctly connected to the device without causing short circuit.

**simple**: Enables the device to supply power to PDs that comply with basic requirements of 802.3af or 802.3at.

**strict**: Enables the device to supply power to PDs that comply with all requirements of 802.3af or 802.3at.

## Modified feature: Enabling recording user IP address conflicts

### Feature change description

As from this release, If the device starts up with the factory defaults, recording user IP address conflicts is enabled.

### Command changes

Modified command: `arp user-ip-conflict record enable`

#### Syntax

```
arp user-ip-conflict record enable
```

```
undo arp user-ip-conflict record enable
```

## Views

System view

## Change description

Before modification: By default, the device starts up with the factory defaults, recording user IP address conflicts is disabled.

After modification: By default, If the device starts up with the factory defaults, recording user IP address conflicts is enabled.

# Modified feature: Enabling IP conflict notification

## Feature change description

As from this release, If the device starts up with the factory defaults, IP conflict notification is disabled.

## Command changes

Modified command: arp ip-conflict log prompt

## Syntax

```
arp ip-conflict log prompt
```

```
undo arp ip-conflict log prompt
```

## Views

System view

## Change description

Before modification: By default, If the device starts up with the factory defaults, IP conflict notification is disabled.

After modification: By default, if the device starts up with the factory defaults, IP conflict notification is enabled.

# Modified feature: Testing the cable connection of an Ethernet interface

## Feature change description

As from this version, the **interface** [ *interface-type interface-number* | *interface-name* ] parameter is added to the **virtual-cable-test** command, and the view where the command is available is changed. The **display virtual-cable-test** command and the **reset interface virtual-cable-test** commands are added.

Modified command: virtual-cable-test

## Old syntax

Layer 2 Ethernet interface view:

**virtual-cable-test**

## New syntax

Any view:

```
virtual-cable-test interface [ interface-type interface-number |  
interface-name ]
```

## Change description

Before modification: This command is supported only in Layer 2 Ethernet interface view. The **interface** *interface-type interface-number* parameter is not supported.

After modification: This command is supported in any view. The **interface** *interface-type interface-number* parameter is supported.

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

## New command: display virtual-cable-test

Use **display virtual-cable-test** to display the cable connection test results of Ethernet interfaces.

## Syntax

```
display virtual-cable-test interface [ interface-type interface-number  
| interface-name ]
```

## 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 this keyword, this command displays the cable connection test results of all Ethernet interfaces.

## Usage guidelines

The test results are for reference only. The maximum length error is 10 meters.

When the obtained cable length is 0 to 3 meters, the length is displayed as **Invalid**.

Interfaces operating at 10 Mbps or 100 Mbps and in up state do not support this command. Fiber ports do not support this command.

When the local interface is shut down, this command is not supported. When the peer interface is shut down, the cable length cannot be obtained.

## Examples

# Display the summary cable connection test results of all Ethernet interfaces.

```
<Sysname> display virtual-cable-test
```

| Interface            | Result         | Length(meters) | Date                |
|----------------------|----------------|----------------|---------------------|
| GigabitEthernet1/0/1 | Not test       |                |                     |
| GigabitEthernet1/0/2 | Abnormal(open) | <50            | 2013-03-06 23:01:34 |

# Display the detailed cable connection test results of Ethernet interface GigabitEthernet 1/0/2.

```
<Sysname> display virtual-cable-test interface GigabitEthernet 1/0/2
```

```

Cable status:
  Pair A length: Invalid meters
  Pair B length: Invalid meters
  Pair C length: Invalid meters
  Pair D length: Invalid meters
  Pair A state: Abnormal(open)
  Pair B state: Abnormal(open)
  Pair C state: Abnormal(open)
  Pair D state: Abnormal(open)
Pair Impedance mismatch: no
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db

```

**Table 1 Command output**

| Field                   | Description                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Result                  | Test result: <ul style="list-style-type: none"> <li>• <b>Abnormal (open)</b>—An open circuit is detected.</li> <li>• <b>Abnormal (short)</b>—A short circuit is detected.</li> <li>• <b>Not test</b>—The test results of the interface are not obtained.</li> </ul>                                                                                    |
| Length(meters)          | Total length of the cable pair, in meters.                                                                                                                                                                                                                                                                                                             |
| Date                    | Time when the test was performed.                                                                                                                                                                                                                                                                                                                      |
| Cable status            | Cable state.                                                                                                                                                                                                                                                                                                                                           |
| Pair x length           | When the cable pair state is <b>OK</b> , this field displays the total length of the cable pair.<br>When the cable pair is in any other state, this field displays the length from the local interface to the faulty point.                                                                                                                            |
| Pair x state            | Cable pair state: <ul style="list-style-type: none"> <li>• <b>OK</b>—The cable pair is in good condition.</li> <li>• <b>Abnormal</b>—The cable pair is abnormal.</li> <li>• <b>Abnormal (open)</b>—An open circuit is detected.</li> <li>• <b>Abnormal (short)</b>—A short circuit is detected.</li> <li>• <b>Invalid</b>—Detection failed.</li> </ul> |
| Pair Impedance mismatch | Pair impedance mismatch: <ul style="list-style-type: none"> <li>• <b>yes</b>—Impedance match.</li> <li>• <b>no</b>—Impedance mismatch.</li> </ul>                                                                                                                                                                                                      |
| Pair skew               | Pair skew.<br>A hyphen (-) is displayed when this test item is not supported.                                                                                                                                                                                                                                                                          |
| Pair swap               | Pair swap.<br>A hyphen (-) is displayed when this test item is not supported.                                                                                                                                                                                                                                                                          |
| Pair polarity           | Pair polarity swap.<br>A hyphen (-) is displayed when this test item is not supported.                                                                                                                                                                                                                                                                 |
| Insertion loss          | Insertion signal loss.                                                                                                                                                                                                                                                                                                                                 |

| Field              | Description                                                                            |
|--------------------|----------------------------------------------------------------------------------------|
|                    | A hyphen (-) is displayed when this test item is not supported.                        |
| Return loss        | Return signal loss.<br>A hyphen (-) is displayed when this test item is not supported. |
| Near-end crosstalk | Near-end crosstalk.<br>A hyphen (-) is displayed when this test item is not supported. |

## Related commands

**virtual-cable-test**

## reset interface virtual-cable-test

Use **reset interface virtual-cable-test** to clear the cable connection test results of Ethernet interfaces.

## Syntax

```
reset interface [ interface-type interface-number | interface-name ]
virtual-cable-test
```

## Views

User view

System view

## Predefined user roles

network-admin

## Parameters

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

## Examples

# Clear the cable connection test results of Ethernet interface GigabitEthernet 1/0/1.

```
<Sysname> reset interface GigabitEthernet 1/0/1 virtual-cable-test
```

## Related commands

**virtual-cable-test**

# Modified feature: Allowing inrush currents of PDs

## Feature change description

As from this release, the command for allowing inrush current of PDs can be configured only in PI view and does not support the **pse** *pse-id* option.

## Command changes

### Modified command: poe high-inrush enable

Use **poe high-inrush enable** to allow high inrush currents of PDs.

Use **undo poe high-inrush enable** to restore the default.

## Old syntax

```
poe high-inrush enable pse pse-id  
undo poe high-inrush enable pse pse-id
```

System view

## New syntax

```
poe high-inrush enable pse pse-id  
undo poe high-inrush enable pse pse-id
```

PoE interface view

## Change description

Before modification: This command can be configured only in system view and cannot be configured in PI view. The **pse *pse-id*** option is supported.

After modification: This command can be configured only in PI view and cannot be configured in system view. The **pse *pse-id*** option is not supported.

**pse *pse-id***: Specifies a PSE by its ID.

# Release 6343P09

This release has the following changes:

- [Modified feature: Factory defaults change for console login and password control settings](#)

## 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
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. Do not edit or delete this file to ensure the authentication and login of the 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 6343

This release has the following changes:

- New feature: Configuring interface alarm functions
- New feature: Configuring the aging timer for temporary MAC address entries for Web authentication
- Modified feature: Displaying the running configuration
- Modified feature: Displaying the running configuration in current view
- Modified feature: 802.1X periodic reauthentication timer
- Modified feature: Periodic MAC reauthentication timer
- Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option of Option 82
- Modified feature: Configuring gRPC collectors
- Modified feature: Displaying detailed information about 802.1X online users

## New feature: Configuring interface alarm functions

### About this task

With the interface alarm functions enabled, when the number of error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

### Restrictions and guidelines

You can configure the error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

An interface that is shut down because of error packet alarms cannot automatically recover. To bring up the interface, execute the **undo shutdown** command on the interface.

### Configuring input error packet alarm parameters

1. Enter system view.

```
system-view
```

2. Configure global input error packet alarm parameters.

```
ifmonitor input-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [ shutdown ]
```

By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packets.

3. Enter Ethernet interface view.

```
interface interface-type interface-number
```

4. Configure input error packet alarm parameters for the interface.

```
port ifmonitor input-error high-threshold high-value low-threshold  
low-value interval interval [ shutdown ]
```

By default, an interface uses the global input error packet alarm parameters.

## Configuring output error packet alarm parameters

1. Enter system view.

```
system-view
```

2. Configure global output error packet alarm parameters.

```
ifmonitor output-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown]
```

By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packets.

3. Enter Ethernet interface view.

```
interface interface-type interface-number
```

4. Configure output error packet alarm parameters.

```
port ifmonitor output-error high-threshold high-value low-threshold  
low-value interval interval [shutdown]
```

By default, an interface uses the global output error packet alarm parameters.

## Command changes

### ifmonitor input-error

Use **ifmonitor input-error** to configure global input error packet alarm parameters.

Use **undo ifmonitor input-error** to restore the default.

#### Syntax

```
ifmonitor input-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown]
```

```
undo ifmonitor input-error slot slot-number
```

#### Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packet alarms.

#### Views

System view

#### Predefined user roles

network-admin

#### Parameters

**high-threshold** *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

**low-threshold** *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

**interval** *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

**shutdown**: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this

keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

**slot** *slot-number*: Specifies an IRF member device by its member ID.

## Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

## Examples

# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms.

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

```
[Sysname] ifmonitor input-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

## Related commands

**snmp-agent trap enable ifmonitor**

## ifmonitor output-error

Use **ifmonitor output-error** to configure global output error packet alarm parameters.

Use **undo ifmonitor output-error** to restore the default.

## Syntax

```
ifmonitor output-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown]
```

```
undo ifmonitor output-error slot slot-number
```

## Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packet alarms.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**high-threshold** *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

**low-threshold** *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

**interval** *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

**shutdown**: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

**slot** *slot-number*: Specifies an IRF member device by its member ID.

## Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

## Examples

# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms.

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

```
[Sysname] ifmonitor output-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

## Related commands

```
snmp-agent trap enable ifmonitor
```

## port ifmonitor input-error

Use **port ifmonitor input-error** to configure input error packet alarm parameters for an interface.

Use **undo port ifmonitor input-error** to restore the default.

## Syntax

```
port ifmonitor input-error high-threshold high-value low-threshold low-value interval interval [ shutdown ]
```

```
undo port ifmonitor input-error
```

## Default

An interface uses the global input error packet alarm parameters.

## Views

Ethernet interface view

## Predefined user roles

network-admin

## Parameters

**high-threshold** *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

**low-threshold** *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

**interval** *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

**shutdown**: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

## Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

## Examples

# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor input-error high-threshold 5000
low-threshold 400 interval 6
```

## Related commands

**snmp-agent trap enable ifmonitor**

## port ifmonitor output-error

Use **port ifmonitor output-error** to configure output error packet alarm parameters for an interface.

Use **undo port ifmonitor output-error** to restore the default.

## Syntax

```
port ifmonitor output-error high-threshold high-value low-threshold low-value interval interval [shutdown]
```

```
undo port ifmonitor output-error
```

## Default

An interface uses the global output error packet alarm parameters.

## Views

Ethernet interface view

## Predefined user roles

network-admin

## Parameters

**high-threshold** *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

**low-threshold** *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

**interval** *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

**shutdown**: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

## Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces. The configuration in interface view takes effect only on the current interface. (Devices that do not support the **slot** keyword.)
- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

## Examples

# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor output-error high-threshold 5000
low-threshold 400 interval 6
```

## Related commands

**snmp-agent trap enable ifmonitor**

## Modified command: snmp-agent trap enable ifmonitor

### Old syntax

```
snmp-agent trap enable ifmonitor [ crc-error ]
undo snmp-agent trap enable ifmonitor [ crc-error ]
```

## New syntax

```
snmp-agent trap enable ifmonitor [ crc-error | input-error | output-error ]  
*  
undo snmp-agent trap enable ifmonitor [ crc-error | input-error |  
output-error ] *
```

## Views

System view

## Change description

Before modification: SNMP notifications for input and output error packets is not supported.

After modification: SNMP notifications for input and output error packets is supported.

# New feature: Configuring the aging timer for temporary MAC address entries for Web authentication

## About this task

If Web authentication is enabled, the device generates a temporary MAC address entry when it detects traffic from a user for the first time. The entry records the MAC address, access interface, and VLAN ID of the user, as well as the aging time of the entry.

The aging timer works as follows:

- If the user does not initiate authentication when the aging timer expires, the device deletes the temporary entry.
- If the user passes authentication before the aging timer expires, the device delete the aging timer and records online information for the Web authentication user.
- If the user fails authentication before the aging timer expires and an Auth-Fail VLAN is specified for Web authentication, the device binds the MAC address of the user to the Auth-fail VLAN and reset the aging timer. If the user still fails authentication when the aging timer expires, the device deletes the temporary entry for the user.

## Restrictions and guidelines

As a best practice, change the aging timer to a bigger value in the following cases:

- Web authentication users without access rights frequently send traffic in a short time. As a result, the access device continuously initiates the web authentication process, increasing the load on the device.
- When a user fails authentication, the user does not have enough time to obtain resources from the Auth-Fail VLAN, for example, it failed to download the virus patches.

## Procedure

1. Enter system view.  
**system-view**
2. Configure the aging timer for temporary MAC address entries.  
**web-auth timer temp-entry-aging** *aging-time-value*  
By default, the aging timer for temporary MAC address entries is 60 seconds.

# Command reference

## New command: web-auth timer temp-entry-aging

Use **web-auth timer temp-entry-aging** to configure the aging timer for temporary MAC address entries.

Use **undo web-auth timer temp-entry-aging** to restore the default.

### Syntax

**web-auth timer temp-entry-aging** *aging-time-value*

**undo web-auth timer temp-entry-aging**

### Default

The aging timer for temporary MAC address entries is 60 seconds.

### Views

System view

### Default command level

network-admin

### Parameters

*aging-time-value*: Specifies the aging timer in seconds for temporary MAC address entries, in the range of 60 to 2147483647.

### Usage guidelines

If Web authentication is enabled, the device generates a temporary MAC address entry when it detects traffic from a user for the first time. The entry records the MAC address, access interface, and VLAN ID of the user, as well as the aging time of the entry.

The aging timer works as follows:

- If the user does not initiate authentication when the aging timer expires, the device deletes the temporary entry.
- If the user passes authentication before the aging timer expires, the device delete the aging timer and records online information for the Web authentication user.
- If the user fails authentication before the aging timer expires and an Auth-Fail VLAN is specified for Web authentication, the device binds the MAC address of the user to the Auth-fail VLAN and reset the aging timer. If the user still fails authentication when the aging timer expires, the device deletes the temporary entry for the user.

As a best practice, change the aging timer to a bigger value in the following cases:

- Web authentication users without access rights frequently send traffic in a short time. As a result, the access device continuously initiates the web authentication process, increasing the load on the device.
- When a user fails authentication, the user does not have enough time to obtain resources from the Auth-Fail VLAN, for example, it failed to download the virus patches.

### Examples

# Set the aging timer for temporary MAC address entries to 500 seconds.

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

```
[Sysname] web-auth timer temp-entry-aging 500
```



Modified command: display web-auth

### Syntax

```
display web-auth [ interface interface-type interface-number ]
```

### Views

Any view

### Change description

The command output added support for the **Temp entry aging time** field.

# Display Web authentication configuration on GigabitEthernet 1/0/1.

```
<Sysname> display web-auth interface gigabitethernet 1/0/1
```

Global Web-auth parameters:

```
Temp entry aging time      : 500 s
HTTP proxy port numbers    : Not configured
HTTPS proxy port numbers   : Not configured
Total online web-auth users : 1
```

GigabitEthernet1/0/1 is link-up

```
Port role                  : Authenticator
Web-auth domain            : my-domain
Auth-Fail VLAN             : Not configured
Offline-detect             : Not configured
Max online users           : 1024
Web-auth enable            : Enabled
Host mode                  : Single-VLAN
Primary Web server         : aaa
Secondary Web server       : Not configured
```

```
Total online web-auth users: 1
```

## Modified feature: Displaying the running configuration

### Feature change description

As from this release, the **display current-configuration** command supports displaying all configuration information.

### Command changes

Modified command: display current-configuration

#### Old syntax

```
display current-configuration [ [ configuration [ module-name ] | interface
[ interface-type [ interface-number ] ] ] | slot slot-number ]
```

#### New syntax

```
display current-configuration [ [ configuration [ module-name ] | interface
[ interface-type [ interface-number ] ] ] [ all ] | slot slot-number ]
```

## Views

System view

## Change description

The **all** keyword was added for the command to support displaying all configuration information.

# Modified feature: Displaying the running configuration in current view

## Feature change description

As from this release, the **display this** command supports displaying all configuration information in current view.

## Command changes

Modified command: display this

### Old syntax

```
display this
```

### New syntax

```
display this [ all ]
```

## Views

System view

## Change description

The **all** keyword was added for the command to support displaying all configuration information in current view.

# Modified feature: 802.1X periodic reauthentication timer

## Feature change description

In this release, the maximum value for the 802.1X periodic reauthentication timer changed from 7200 to 86400.

## Command changes

Modified command: dot1x timer reauth-period (system view)

### Syntax

```
dot1x timer reauth-period reauth-period-value
```

### Views

System view

## Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in system view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in system view.

## Modified command: dot1x timer reauth-period (interface view)

### Syntax

```
dot1x timer reauth-period reauth-period-value
```

### Views

Layer 2 Ethernet interface view

## Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in interface view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in interface view.

# Modified feature: Periodic MAC reauthentication timer

## Feature change description

In this release, the maximum value for the periodic MAC reauthentication timer changed from 7200 to 86400.

## Command changes

## Modified command: mac-authentication timer (system view)

### Syntax

```
mac-authentication timer reauth-period reauth-period-value
```

### Views

System view

## Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in system view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in system view.

## Modified command: mac-authentication timer (interface view)

### Syntax

```
mac-authentication timer reauth-period reauth-period-value
```

### Views

Layer 2 Ethernet interface view

## Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in interface view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in interface view.

## Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option of Option 82

### Feature change description

As from this release, you can configure the **hex** *remote-id* option when you configure the padding mode and padding format for the Remote ID sub-option of Option 82.

### Command changes

#### Modified command: dhcp relay information remote-id

##### Old syntax

```
dhcp relay information remote-id { normal [ format { ascii | hex } ] | string  
remote-id | sysname }
```

##### New syntax

```
dhcp relay information remote-id { hex remote-id | normal [ format { ascii |  
hex } ] | string remote-id | sysname }
```

##### Views

Interface view

## Change description

Before modification: The **hex** *remote-id* option is not supported in this command.

After modification: The **hex** *remote-id* option is supported in this command.

## Parameters

**hex** *remote-id*: Pads the Remote ID sub-option with a user-defined hexadecimal string of 2 to 256 characters. The number of characters in the string must be even.

## Modified feature: Configuring gRPC collectors

### Feature change description

As from this release, you can add collectors to a destination group by their domain names. When you specify collectors by their domain names, use the following restrictions and guidelines:

- You must configure DNS to make sure the device can translate the domain names of the collectors to IP addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

- To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device will push data to the first reachable IP address.

## Command changes

### New command: domain-name

Use **domain-name** to add the domain name of an IPv4 collector to a destination group.

Use **undo domain-name** to remove the domain name of an IPv4 collector from a destination group.

#### Syntax

```
domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
undo domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
```

#### Default

A destination group does not contain IPv4 collectors.

#### Views

Destination group view

#### Predefined user roles

network-admin

#### Parameters

**domain-name**: Domain name mapped to the IPv4 address of a collector. It can be a case-insensitive string of 1 to 253 characters and can contain letters, digits, hyphens (-), and dots (.).

**port** *port-number*: Specifies the service port number on which the collector receives data. The value range is 1 to 65535 and the default is 50051. To have the collector receive data, make sure the specified service port number is the same as the one used on the collector.

**vpn-instance** *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the collector belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Make sure the specified VPN instance already exists. If the collector is on the public network, do not specify this option.

**tls**: Enables Transport Layer Security (TLS) to encrypt the gRPC connection between the device and the specified collector. The device will then use a root TLS certificate that came with it for encryption. By default, the gRPC connection between the device and a collector is unencrypted.

#### Usage guidelines

If you specify collectors by their domain names, you must configure DNS to make sure the device can translate the domain names of the collectors to IPv4 addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device will push data to the first reachable IP address.

To add multiple collectors, repeat this command.

A collector is uniquely identified by a three-tuple of domain name, port number, and VPN instance name. One collector must have a different domain name, port number, or VPN instance name than the other collectors.

If you execute this command multiple times to change the TLS enabling state for a collector, the most recent configuration takes effect.

A destination group can have a maximum of five collectors.

You can enable TLS encryption globally by executing the **grpc pki domain** command in system view or enable collector-specific TLS encryption by specifying the **tls** keyword when you specify the collector. For a collector, the setting in system view has higher priority than the collector-specific setting.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

## Examples

# Add the IPv4 collector at **sample.com** to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] domain-name sample.com
```

## Related commands

**destination-group** (subscription view)

**subscription**

**display dns host** (*Layer 3—IP Services Command Reference*)

## New command: ipv6 domain-name

Use **ipv6 domain-name** to add the domain name of an IPv6 collector to a destination group.

Use **undo ipv6 domain-name** to remove the domain name of an IPv6 collector from a destination group.

## Syntax

```
ipv6 domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
```

```
undo ipv6 domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
```

## Default

A destination group does not contain IPv6 collectors.

## Views

Destination group view

## Predefined user roles

network-admin

## Parameters

**domain-name**: Domain name mapped to the IPv6 address of a collector. It can be a case-insensitive string of 1 to 253 characters and can contain letters, digits, hyphens (-), and dots (.).

**port** *port-number*: Specifies the service port number on which the collector receives data. The value range is 1 to 65535 and the default is 50051. To have the collector receive data, make sure the specified service port number is the same as the one used on the collector.

**vpn-instance** *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the collector belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31

characters. Make sure the specified VPN instance already exists. If the collector is on the public network, do not specify this option.

**tls**: Enables Transport Layer Security (TLS) to encrypt the gRPC connection between the device and the specified collector. The device will then use a root TLS certificate that came with it for encryption. By default, the gRPC connection between the device and a collector is unencrypted.

## Usage guidelines

If you specify IPv6 collectors by their domain names, you must configure DNS to make sure the device can translate the domain names of the collectors to IPv6 addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device will push data to the first reachable IP address.

To add multiple collectors, repeat this command.

A collector is uniquely identified by a three-tuple of domain name, port number, and VPN instance name. One collector must have a different domain name, port number, or VPN instance name than the other collectors.

If you execute this command multiple times to change the TLS enabling state for a collector, the most recent configuration takes effect.

A destination group can have a maximum of five collectors.

You can enable TLS encryption globally by executing the **grpc pki domain** command in system view or enable collector-specific TLS encryption by specifying the **tls** keyword when you specify the collector. For a collector, the setting in system view has higher priority than the collector-specific setting.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

## Examples

# Add the IPv6 collector at **sample.com** to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv6 domain-name sample.com
```

## Related commands

**destination-group** (subscription view)

**subscription**

**display dns host** (Layer 3—IP Services Command Reference)

## Modified command: display grpc

### Syntax

```
display grpc [ verbose ]
```

### Views

Any view

### Change description

Before modification: The output from this command contains the **Encoding** and **Telemetry data mode** field. However, the command output does not contain the **Domain name** field.

After modification: The **Domain name** field is available in the command output. The **Encoding** and **Telemetry data mode** fields are not available in the command output.

## Modified feature: Displaying detailed information about 802.1X online users

### Feature change description

As from this version, the **display dot1x connection** command can display the AAA authentication method used by each user when they come online.

### Command changes

#### Modified command: display dot1x connection

##### Syntax

```
display dot1x connection [ open ] [ interface interface-type  
interface-number | slot slot-number | user-mac mac-address | user-name  
name-string ]
```

##### Views

Any view

##### Change description

The **AAA authentication method** field was added to the command output. The value for this field can be **Local**, **HWTACACS**, **RADIUS**, or **None**.

The following shows an example:

# Display information about all 802.1X online users.

```
<Sysname> display dot1x connection
```

```
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```
User access state: Successful
```

```
Authentication domain: aaa
```

```
IPv4 address: 192.168.1.1
```

```
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
```

```
Authentication method: CHAP
```

```
AAA authentication method: Local
```

```
Initial VLAN: 1
```

```
Authorization untagged VLAN: 6
```

```
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33  
35 37 40 to 100
```

```
Authorization ACL number/name: 3001
```

```
Authorization dynamic ACL name: N/A
```

```
Authorization user profile: N/A
```

```
Authorization CAR: N/A
```

```
Authorization URL: N/A
```



Termination action: Default  
Session timeout period: 2 s  
Online from: 2013/03/02 13:14:15  
Online duration: 0h 2m 15s

# Release 6337P01

This release has the following changes:

- New feature: Configuring SmartMC
- New feature: Configuring interface alarm functions
- New feature: Configuring Option 60 for DHCP requests
- New feature: Configuring the type of port ID TLVs advertised by LLDP
- New feature: Enabling displaying LLDP local information about all interfaces
- New feature: PoE forced power supply
- New feature: Interval at which the SNMP module examines the system configuration for changes
- New feature: Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users
- New feature: Automated IPv6 underlay network deployment for VCF fabric
- Modified feature: Setting the port status detection timer
- Modified feature: 802.1X EAD assistant
- Modified feature: Displaying information about online MAC authentication users
- Modified feature: L2PT for CFD

## New feature: Configuring SmartMC

### About SmartMC

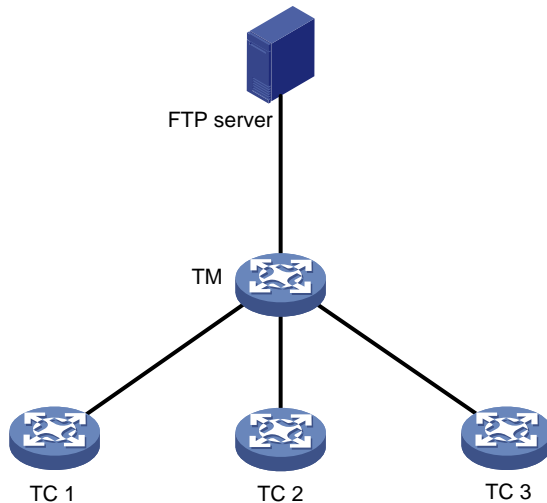
Smart Management Center (SmartMC) centrally manages and maintains dispersed network devices at network edges. In a SmartMC network, only one device acts as the commander and the remaining devices all act as members. SmartMC provides the following features for you to manage the members from the commander:

- Configuration file backup and download.
- Software upgrade.
- Configuration deployment.
- Faulty member replacement.

### SmartMC network framework

Figure 1 shows the basic framework of a SmartMC network.

**Figure 3** SmartMC network framework



The SmartMC network contains the following elements:

- **Commander**—Also called topology master (TM), which manages all members in the SmartMC network.
- **Member**—Also called topology client (TC), which is managed by the commander.
- **File server**—Stores startup software images and configuration files for the commander and members.

## SmartMC network establishment

A SmartMC network can be established automatically or manually. In an automatically established SmartMC network, the commander obtains member information through NETCONF sessions to form the network topology. The member information includes port information, LLDP neighbor information, STP information, device type, and software version. In a manually established SmartMC network, the commander obtains member's LLDP neighbor information through NETCONF sessions and member's hardware information through SNMP Get operations.

### Automatic SmartMC network establishment

The commander and members use the following procedure to establish a SmartMC network:

1. After SmartMC is enabled, the commander broadcasts a SmartMC packet at an interval of 15 seconds to detect members in the network. The SmartMC packet contains information of the commander, such as its bridge MAC address and the IP address of VLAN-interface 1.
2. When a member receives the packet, it records the commander information, and returns a response packet to the commander. The response packet contains information of the member, such as its bridge MAC address and the IP address of VLAN-interface 1.
3. When the commander receives the response packet, it initiates a NETCONF session to the member with the default username **admin** and the default password **admin**. The commander then obtains detailed information about the member through the session, including port information, LLDP neighbor information, STP information, device type, and software version.
4. The commander establishes a connection to the member for tracking the liveliness of the member, and adds the member to the SmartMC network.
5. Based on the LLDP neighbor information obtained from all members, the commander forms a SmartMC topology.

After the SmartMC network is established, the commander and members check for the existence of each other by exchanging SmartMC packets.

- When a member receives a SmartMC broadcast packet from the commander, it compares the bridge MAC address in the packet with the recorded bridge MAC address. If the two bridge MAC addresses are the same, the member returns a response packet to the commander. If the member does not receive a broadcast packet from the commander within the time limit, the member determines that the commander does not exist in the network anymore. Then, the member clears the commander information. The time limit is a random value in the range of 60 to 120 seconds.
- When the commander receives a response packet from a member, it compares the bridge MAC address in the packet with the recorded bridge MAC address. If the two bridge MAC addresses are the same, the commander determines that the member still exists in the network. If the commander does not receive a response packet from a member within 150 seconds, the commander determines that the member is offline. Then, the commander sets the status of the member to offline.

## Manual SmartMC network establishment

You can log in to the Web interface of the commander, and enter the IP address, username, and password of the members to manually add them to the network. The members can join the network without exchanging SmartMC packets with the commander. For more information, see *Comware 7 Web-Based Products User Guide*.

After you specify the information of a member on the commander, the commander performs the following operations to add the member to the network:

- Verify that the member can be accessed through Telnet.
- Obtain basic member information, including LLDP neighbor information through NETCONF.
- Obtain hardware information through SNMP Get operations.

## SmartMC features

### Bulk configuration deployment for members

This feature allows you to deploy multiple command lines to members from the commander, eliminating the need to log in to members and configure the command one by one.

The procedure for bulk configuration deployment is as follows:

1. The commander acts as a Telnet client and establishes Telnet connections to the members.
2. The commander deploys a batch file to the members through Telnet connections. The batch file is created on the commander and contains command lines to be deployed.
3. The members run the command lines in the file.

### Bulk configuration deployment for ports connecting APs and IP phones

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration.

When the commander first detects the association of an AP or IP phone on a port through LLDP, it deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

If the AP or IP phone disconnects from the port, the configurations on the port remain. When a new device comes online from the port, configurations used by the port depend on the new device type.

- If the new device is an AP or IP phone and has the same type as the disconnected device, the configurations on the port remain unchanged.
- If the new device is an AP or IP phone but has a different type as the disconnected device, the commander deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.
- If the new device is neither an AP nor an IP phone, the configurations on the port remain unchanged.

To disable the commander from deploying a batch file to ports, remove the specified batch file or execute the `undo smartmc batch-file-apply enable` command to disable batch file deployment.

## Configuration file backup

You can use the following methods to back up the next-startup configuration file on the commander and members:

- **Automatic backup**—Enable this feature for the commander and all members in the network to immediately perform a backup. After that, the commander and members back up the configuration file at a user-specified interval.
- **Manual backup**—Manually trigger a backup on the commander or the specified members or SmartMC groups.

To back up the configuration file on a member, the commander instructs the member by unicasting a SmartMC packet to them. When a member receives the packet, it saves the running configuration to the next-startup configuration file and uploads the file to the file server.

## Startup software and configuration file upgrade

This feature enables users to upgrade startup software and the configuration file of member devices from the commander.

Before upgrade, you must upload the upgrade files from the commander to the file server and specify the upgrade files on the file server for the members to download.

The procedure for startup software and configuration file upgrade is as follows:

1. The commander instructs the members (or SmartMC group) to download the upgrade files from the file server.
2. The members download the upgrade files from the file server.
3. The members upgrade the startup software and configuration file as follows:
  - **Startup software upgrade**—Uses the boot loader method to perform the software upgrade. The members might be restarted during the upgrade process.
  - **Configuration file upgrade**—Replaces the current configuration file with the upgrade configuration file. The members will not be restarted during the upgrade process.

## Faulty member replacement

You can use the following methods to replace a faulty member:

- **Automatic replacement**—Enables the commander to record the positions of all members in the topology for replacement. When the commander discovers that the new member has physically replaced the faulty member, it compares the new member with the faulty one. The commander performs a replacement if the following requirements are met:
  - The new member is deployed at the same topological position as the faulty one.
  - The models of the new member and faulty member are the same.

The commander then instructs the new member to download the configuration file of the faulty member from the file server. After downloading the configuration file, the new member runs the configuration file to complete the replacement.

- **Manual replacement**—After the faulty member is physically replaced, you manually trigger a configuration replacement. The new member will download the configuration file of the faulty member from the file server and run the file to complete the replacement.

## Outgoing interface for a SmartMC network

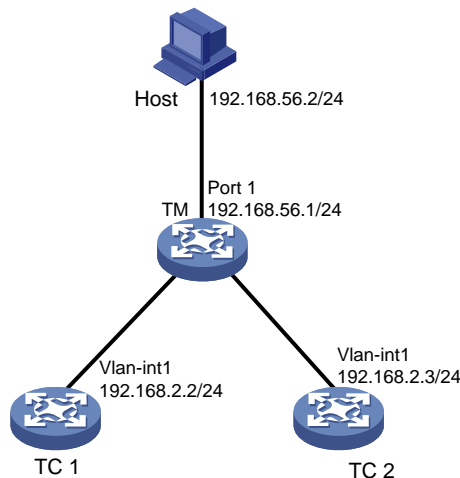
The outgoing interface feature allows hosts connecting to an outgoing interface to access all the members in a SmartMC network. You can configure multiple outgoing interfaces for a SmartMC network.

As shown in [Figure 2](#), the host is connected to port 1 on the TM and TC 1 and TC 2 are in a different network segment than the host. The host can access the Web interface of the TM but cannot access the Web interface of any member.

If port 1 on the TM is configured as the outgoing interface, the system mirrors the IP address of each member to a new address. The new address contains the IP address of the outgoing interface and the port number assigned by the commander to the member in the format of *IP address:Port number*. This enables the host to access the Web interfaces of members from the Web interface of the TM.

To access the Web interface of a member, enter the Web interface of the commander, and click **Visibility** from the navigation pane. Then, click the **Topology** tab, select the target member, and click **Login to Web interface**.

**Figure 4 SmartMC network**



## Automatic link aggregation

Automatic link aggregation automatically bundles multiple physical Ethernet links between two members into one logical link, called an aggregate link. This feature provides increased link bandwidth and improved link reliability.

---

### NOTE:

- Automatic link aggregation cannot be performed between the commander and a member, or between a member and a device outside the SmartMC network. You can aggregate the links between the commander and a member manually. For more information about manual link aggregation, see Ethernet link aggregation in *Layer 2—LAN Switching Configuration Guide*.
  - If a member enabled with automatic link aggregation joins a SmartMC network whose commander is disabled with the aggregation feature, the feature will be disabled for the member as well. This might affect service traffic forwarding on the member.
- 

## VLAN creation for members

To simplify configuration and management, you can create a VLAN for members. Then, all access ports on a member that are not connected to other members or the commander are assigned to the VLAN.

If a member has access ports that are connected to offline devices, you must remove the offline devices before creating a VLAN for the member.

The VLAN creation fails for a member if one or more access ports cannot be assigned to the VLAN. If the VLAN creation fails, the VLAN memberships for the access ports are restored to the state before the VLAN was created.

The failure to create a VLAN for a member does not affect the VLAN creation for other members.

## Resource monitoring

Resource monitoring allows you to view resource usage, memory usage, temperature information, and packet dropping information of commanders and members on the commander.

You can view the usage and temperature information on the commander, and view packet dropping information from the **SmartMC > Intelligent O&M > Resource monitoring** page of the commander's Web interface.

## Restrictions: Hardware compatibility with SmartMC

The HPE 5140 EI switch series cannot act as the commander. The switches only support SmartMC members.

## Restrictions and guidelines: SmartMC configuration

You need to enable SmartMC on both the commander and members and perform all the other tasks only on the commander.

The following features take effect only on members added to the SmartMC network automatically:

- Configuration file backup.
- Faulty member replacement.
- Startup software and configuration file upgrade.
- Automatic link aggregation.

A SmartMC network is established in VLAN 1. For the network to work correctly, do not configure security settings in VLAN 1.

## SmartMC tasks at a glance

To configure SmartMC, perform the following tasks:

1. [Enabling SmartMC](#)

2. [Setting the file server information](#)

This task is required for configuring automatic configuration file backup, replacing faulty members, and upgrading the startup software and configuration file on members.

3. (Optional.) [Configuring an outgoing interface for the SmartMC network](#)

4. (Optional.) [Enabling automatic Ethernet link aggregation](#)

5. (Optional.) [Modifying the password of the default user for members](#)

6. [Creating a SmartMC group](#)

This task is required for upgrading the startup software and configuration file on members and deploying a batch file to a SmartMC group.

7. (Optional.) Deploying and managing configuration

- [Creating a VLAN for members](#)
- [Deploying a batch file to members](#)
- [Configuring a batch file for ports connecting APs or IP phones](#)
- [Backing up configuration files](#)

8. (Optional.) Monitoring and maintaining the SmartMC network

- [Configuring resource monitoring](#)
- [Upgrading the startup software and configuration file on members](#)
- [Managing the network topology](#)
- [Replacing faulty members](#)

# Prerequisites for SmartMC

Before you configure SmartMC, perform the following tasks on the commander and members:

- Enable the Telnet service, and configure scheme authentication for VTY user lines. For information about Telnet service and VTY user lines, see CLI login configuration in *Fundamentals Configuration Guide*.
- Configure a local user.
  - Specify the username and password.
    - On the commander, the username and password must be the same as the username and password configured by using the **smartmc tm username username password { cipher | simple } string enable** command.
    - On a member, set both the username and password to **admin**, and execute the **password-control length 4 password-control composition type-number 1 type-length 1**, and **undo password-control complexity user-name check** commands to lower the password complexity requirements.

This is because SmartMC requires that the commander use username **admin** and password **admin** to communicate with members, which does not meet the default password complexity requirements. For more information about these commands, see password control commands in *Security Command Reference*.

After the SmartMC network is established, you can increase the password complexity requirements and use the **smartmc tc password** command to modify the username and password.
  - Specify the Telnet, HTTP, and HTTPS services for the user.
  - Set the RBAC role of the local user to network-admin.

For information about local users, see AAA configuration in *Security Configuration Guide*. For information about user roles, see RBAC configuration in *Fundamentals Configuration Guide*.

- Enable NETCONF over SOAP over HTTP. For information about NETCONF over SOAP, see NETCONF configuration in *Network Management and Monitoring Configuration Guide*.
- Enable LLDP globally. For information about LLDP, see *Layer 2—LAN Switching Configuration Guide*.
- To manage the commander and members through a Web interface, you must enable the HTTP and HTTPS services, and set the service type to HTTP and HTTPS for the local user. For information about Web login, HTTP, and HTTPS, see *Fundamentals Configuration Guide*.
- To manually establish a SmartMC network, you must configure the **snmp-agent community read public** and **snmp-agent sys-info version v2c** commands on the members. For information about SNMP, see *Network Management and Monitoring Configuration Guide*.

## Enabling SmartMC

### About SmartMC

Enable this feature on both the commander and members to enable management of members from the commander.

### Restrictions and guidelines

A SmartMC network must have one and only one commander.

If you change the role of the commander to member or disable SmartMC on the commander, all SmartMC settings in its running configuration will be cleared.

SmartMC fails to be enabled if ACL resources are insufficient. If ACL resources are insufficient, use the **undo acl** command to delete unnecessary ACLs and then enable SmartMC. You can execute



the **display acl** command to view ACL configuration and match statistics. For more information about ACLs, see *ACL and QoS Configuration Guide*.

SmartMC fails to be enabled if ports 80 and 443 have been used.

If you execute the **smartmc enable** command multiple times, the most recent configuration takes effect. You can execute the command to change the device role or the password.

## Procedure

1. Enter system view.  
**system-view**
2. Enable SmartMC and set the device role.  
**smartmc { tc | tm username *username* password { cipher | simple } string } enable**  
By default, SmartMC is disabled.

## Setting the file server information

### About files stored on the file server

In a SmartMC network, a file server is used to store the following files:

- Upgrade startup software files and upgrade configuration file for members.
- Backup configuration files of the commander and members.

For information about FTP servers, see configuring FTP in *Fundamentals Configuration Guide*. For information about SFTP servers, see configuring SSH in *Security Configuration Guide*.

### Restrictions and guidelines

You can use the following methods to specify a file server:

- Specify the IP address of a file server.
- Specify the IP address of the commander. The commander will act as a file server.

To configure the commander to act as a file server, make sure the commander has enough storage space for storing the files required by members.

To use an independent file server, connect the file server to the commander instead of the members as a best practice. The file server uses VLAN 1 to communicate with the SmartMC network. If you connect the file server to members, creating a VLAN for members will assign member interfaces connecting to the file server to the created VLAN, causing file server disconnection. For more information about member VLAN creation, see "[Creating a VLAN for members](#)."

## Procedure

1. Enter system view.  
**system-view**
2. Set the file server information.  
**smartmc { ftp-server | sftp-server } { ipv4-address | ipv6 *ipv6-address* } [ port *port* ] [ vpn-instance *vpn-instance-name* ] [ directory *directory* ] username *username* password { cipher | simple } *string***  
By default, no file server information is set.

# Configuring an outgoing interface for the SmartMC network

## Restrictions and guidelines

VLAN interface 1 cannot be used as an outgoing interface, because the SmartMC network is established in VLAN 1.

## Procedure

1. Enter system view.  
**system-view**
2. Enter VLAN interface view.  
**interface vlan** *interface-number*
3. Configure the interface as an outgoing interface.  
**smartmc outbound**

By default, no interface is used as an outgoing interface.

# Enabling automatic Ethernet link aggregation

## Restrictions and guidelines

Enabling or disabling automatic link aggregation might cause network flapping, and the members might go offline for a short period of time.

## Procedure

1. Enter system view.  
**system-view**
2. Enable automatic Ethernet link aggregation.  
**smartmc auto-link-aggregation enable**

By default, automatic Ethernet link aggregation is disabled.

# Modifying the password of the default user for members

## About modifying the password of the default user for members

During SmartMC network establishment, the commander uses the default username and password to establish NETCONF sessions to members automatically added to the network. The default username and password of the members for NETCONF session establishment are **admin** and **admin**.

To enhance security, you can perform this task to change the password for the default user **admin** of the members after the commander adds the members to the network.

## Restrictions and guidelines

Do not modify the password for members that are manually added to the SmartMC network. If you modify the password for a manually added member, you will not be able to manage that member from the commander.

You can use the **display smartmc tc verbose** command to identify the method used to add the members.

## Procedure

1. Enter system view.  
**system-view**

2. Modify the password of the default user for members.

```
smartmc tc password [cipher] string
```

## Creating a SmartMC group

### About SmartMC groups

This feature allows you to create a SmartMC group on the commander and add members to the group. When you perform the following operations, you can specify a SmartMC group to apply the operations to all members in the group:

- Startup software upgrade.
- Configuration file upgrade.
- Configuration deployment.

### Procedure

1. Enter system view.

```
system-view
```

2. Create a SmartMC group and enter its view.

```
smartmc group group-name
```

3. (Optional.) Display predefined device types.

```
match device-type ?
```

If the device type of the members is not predefined on the commander, you must manually add the device type to the commander. This enables members of an undefined type to join a SmartMC group created on the commander.

4. Set a match criterion.

```
match { device-type device-type | ip-address ip-address  
{ ip-mask-length | ip-mask } | mac-address mac-address mac-mask-length }
```

By default, no match criterion is set.

5. If the device type of the members is not predefined on the commander, perform the following tasks to manually define the device type on the commander:

- a. Return to system view.

```
quit
```

- b. Define a device type on the commander.

```
smartmc tc sysoid sysoid device-type device-type
```

To obtain the SYSOID of a member, execute the **display smartmc tc verbose** command.

You cannot define a predefined member type as another type.

## Creating a VLAN for members

### Restrictions and guidelines

If you perform this task multiple times to create a VLAN for members, the most recent configuration takes effect.

### Procedure

1. Enter system view.

```
system-view
```

2. Creating a VLAN for members and assign access ports on the members to the VLAN.

```
smartmc vlan vlan-id { group group-name-list | tc tc-id-list }
```

## Deploying a batch file to members

1. Execute the following command in user view to create a batch file and edit the command lines to be deployed to members.

```
create batch-file cmd-filename
```

Each command occupies a line in the batch file. When you finish editing, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

2. Enter system view.

```
system-view
```

3. Deploy the batch file to a list of members or SmartMC groups.

```
smartmc batch-file cmd-filename deploy { group group-name-list | tc tc-id-list }
```

## Configuring a batch file for ports connecting APs or IP phones

### Restrictions and guidelines

All commands in the batch file must be commands used in interface view.

The size of the batch file cannot exceed 8190 characters.

Make sure the file name is correct when specifying the batch file because the system does not verify whether the file name is correct. After specifying the batch file, do not delete the file or rename the file.

### Procedure

1. (Optional.) Execute the following command in user view to create a batch file and edit the command lines to be deployed to members.

```
create batch-file cmd-filename
```

Each command occupies a line in the batch file. When you finish editing, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

2. Enter system view.

```
system-view
```

3. Specify the batch file for ports connecting APs or IP phones.

```
smartmc batch-file batch-file-name apply { ap | phone }
```

4. (Optional.) Disable batch file deployment.

```
undo smartmc batch-file-apply enable
```

By default, batch file deployment is enabled.

## Backing up configuration files

### About backing up configuration files

Perform this task to back up the configuration file of the commander or the specified members. Configuration files automatically backed up to the file server are named in the format of *device bridge MAC address\_backup.cfg*.

## Restrictions and guidelines

When you change the commander in the SmartMC network, make sure the backup configuration file of the original commander on the file server is deleted. If the file still exists, the new commander might download the file and run the settings. This will cause a conflict in the network.

The maximum number of members that can perform automatic configuration at the same time is limited by the performance of the file server. If automatic configuration backup fails, set the maximum number of members to a smaller value.

## Prerequisites

Before performing this task, you must set the file server information (see "[Setting the file server information](#)").

## Procedure

1. Enter system view.

```
system-view
```

2. Set the maximum number of members that can perform configuration file backup at the same time.

```
smartmc backup configuration max-number max-number
```

By default, a maximum of five members can perform automatic configuration backup at the same time.

3. Back up configuration files.

Choose one option as needed:

- o Enable automatic configuration file backup and set the backup interval.

```
smartmc backup startup-configuration interval interval-time
```

By default, automatic configuration file backup is disabled.

- o Manually back up the configuration file on members.

```
smartmc backup configuration { group group-name-list | tc
[ tc-id-list ] }
```

TC ID 0 represents the commander.

## Configuring resource monitoring

1. Enter system view.

```
system-view
```

2. Set the interval for the commander to obtain resource monitoring information.

```
smartmc resource-monitor interval interval
```

The default setting is 1 minute.

3. Set the aging time for resource monitoring information.

```
smartmc resource-monitor max-age max-age
```

The default setting is 24 hours.

4. Enable resource monitoring.

```
smartmc resource-monitor [ cpu | memory | packet-drop | temperature ] *
[ group group-name-list | tc { tc-id-list | mac-address mac-address } | tm ]
```

By default, resource monitoring is disabled.

If you do not specify a resource type, this command enables resource monitoring for all resource types.

If you do not specify a device to monitor (member or commander), this command enables resource monitoring on the commander and all members.

# Upgrading the startup software and configuration file on members

## About upgrading the startup software and configuration file on members

You can use the following methods to upgrade the startup software and configuration file on members:

- Schedule an upgrade by specifying an upgrade time or upgrade delay.
- Upgrade immediately by not specifying an upgrade time or upgrade delay.

## Restrictions and guidelines for startup software and configuration file upgrade

A member can perform only one upgrade task at a time.

An immediate upgrade cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

## Prerequisites

Before performing this task, you must set the file server information (see "[Setting the file server information](#)").

## Upgrading the startup software and configuration file on members

### Upgrading the startup software and configuration file in one step

1. Enter system view.  
**system-view**
2. Upgrade the startup software on members in one step.  
**smartmc upgrade boot-loader tc** { *tc-id-list* { **boot** *boot-filename* **system** *system-filename* | **file** *ipe-filename* } } <1-40> [ **delay** *delay-time* | **time** *in-time* ]

---

#### CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

---

3. Upgrade the configuration file on members in one step.  
**smartmc upgrade startup-configuration tc** { *tc-id-list* *cfg-filename* } <1-40> [ **delay** *delay-time* | **time** *in-time* ]

---

#### CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

---

### Configuring startup software and configuration file upgrade step by step

1. Enter system view.  
**system-view**
2. Configure startup software upgrade for members step by step:
  - a. Specify the upgrade startup software files.

```
smartmc tc tc-id boot-loader { ipe-filename | boot boot-filename system system-filename }
```

- b. Upgrade the startup software on members.

```
smartmc upgrade boot-loader tc tc-id-list
```

---

**△ CAUTION:**

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

---

3. Configure configuration file upgrade for members step by step:

- a. Specify the upgrade configuration file.

```
smartmc tc tc-id startup-configuration cfg-filename
```

- b. Upgrade the configuration file on members.

```
smartmc upgrade startup-configuration tc tc-id-list
```

---

**△ CAUTION:**

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

---

## Upgrading the startup software and configuration file on all members in SmartMC groups

### Upgrading the startup software and configuration file in one step

1. Enter system view.

```
system-view
```

2. Upgrade the startup software on all members in SmartMC groups in one step.

```
smartmc upgrade boot-loader group { group-name-list [ boot boot-filename system system-filename | file ipe-filename ] }&<1-40>  
[ delay minutes | time in-time ]
```

---

**△ CAUTION:**

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

---

3. Upgrade the configuration file on all members in SmartMC groups in one step.

```
smartmc upgrade startup-configuration group { group-name-list file cfg-filename }&<1-40> [ delay minutes | time in-time ]
```

---

**△ CAUTION:**

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

---

### Configuring startup software and configuration file upgrade step by step

1. Enter system view.

```
system-view
```

2. Enter SmartMC group view.

**smartmc group** *group-name*

3. Specify the upgrade startup software files for the SmartMC group.

**boot-loader file** { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

By default, no upgrade startup software files are specified for a SmartMC group.

4. Specify the upgrade configuration file for the SmartMC group.

**startup-configuration** *cfgfile*

By default, no upgrade configuration file is specified for a SmartMC group.

5. Return to system view.

**quit**

6. Upgrade the startup software and configuration file on all members in the SmartMC group.

Choose one option as needed:

- Upgrade the startup software.

**smartmc upgrade boot-loader group** *group-name-list* [ **delay** *minutes* | **time** *in-time* ]

---

**△ CAUTION:**

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

---

- Upgrade the configuration file.

**smartmc upgrade startup-configuration group** *group-name-list* [ **delay** *minutes* | **time** *in-time* ]

---

**△ CAUTION:**

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

---

## Managing the network topology

### Refreshing the network topology

#### About refreshing the network topology

You can use the following methods to refresh the network topology:

- **Automatic topology refresh**—Specify the refresh interval to allow the commander to refresh the network topology periodically.
- **Manual topology refresh**—Execute the **smartmc topology-refresh** command to manually refresh the network topology.

#### Restrictions and guidelines

The topology refresh time depends on the number of members in the network.

#### Procedure

Choose one option as needed:

- Manually refresh the network topology in any view.

**smartmc topology-refresh**



- Configure automatic network topology refresh.
  - a. Enter system view.
 

```
system-view
```
  - b. Set the automatic topology refresh interval.
 

```
smartmc topology-refresh interval interval
```

By default, the automatic topology refresh interval is 60 seconds.

## Saving the network topology

### About saving the network topology

This task allows you to save the current network topology to the **topology.db** file in the flash memory. After the commander reboots, it uses the **topology.db** file to restore the network topology.

#### Procedure

1. Enter system view.
 

```
system-view
```
2. Save the network topology.
 

```
smartmc topology-save
```

## Replacing faulty members

### Restrictions and guidelines

Make sure the new member for replacement and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Make sure the new member has a different member ID than all the members in the SmartMC network, including offline members. Faulty members are considered offline.

To automatically replace a faulty member, first enable automatic replacement, and then install the new member at the location where the faulty member was installed and connect all cables.

To manually replace a faulty member, first install the new member at the location where the faulty member was installed, connect all cables, and then execute the manual replacement command.

#### Prerequisites

Before you replace a faulty member, set the file server information (see "[Setting the file server information](#)").

#### Procedure

1. Enter system view.
 

```
system-view
```
2. Replace faulty members.
 

Choose one option as needed:

  - Enable automatic faulty member replacement.
 

```
smartmc auto-replace enable
```

By default, automatic faulty member replacement is disabled.
  - Manually replace a faulty member.
 

```
smartmc replace tc tc-id1 faulty-tc tc-id2
```

# Display and maintenance commands for SmartMC

Execute **display** commands in any view.

| Task                                                            | Command                                                                                                            |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Display the backup status on members.                           | <b>display smartmc backup configuration status</b>                                                                 |
| Display the batch file execution results.                       | <b>display smartmc batch-file status</b> [ap   last <i>number</i> / phone ]                                        |
| Display SmartMC configuration.                                  | <b>display smartmc configuration</b>                                                                               |
| Display connections between the devices in the SmartMC network. | <b>display smartmc device-link</b>                                                                                 |
| Display SmartMC group information.                              | <b>display smartmc group</b> [ <i>group-name</i> ] [verbose ]                                                      |
| Display the faulty member replacement status.                   | <b>display smartmc replace status</b>                                                                              |
| Display resource monitoring information.                        | <b>display smartmc resource-monitor</b> [ cpu   memory   temperature ] * [ tc <i>tc-id</i>   tm ]                  |
| Display resource monitoring configuration.                      | <b>display smartmc resource-monitor configuration</b>                                                              |
| Display member information.                                     | <b>display smartmc tc</b> [ <i>tc-id</i> ][verbose ]                                                               |
| Display log information in the log buffer on a member.          | <b>display smartmc tc</b> <i>tc-id</i> log buffer [ module <i>module-name</i> [ mnemonic <i>mnemonic-value</i> ] ] |
| Display restart log information for a member.                   | <b>display smartmc tc</b> <i>tc-id</i> log restart                                                                 |
| Display VLAN creation results for members.                      | <b>display smartmc vlan</b>                                                                                        |
| Display member upgrade status.                                  | <b>display smartmc upgrade status</b>                                                                              |

## SmartMC configuration examples

### Example: Configuring SmartMC

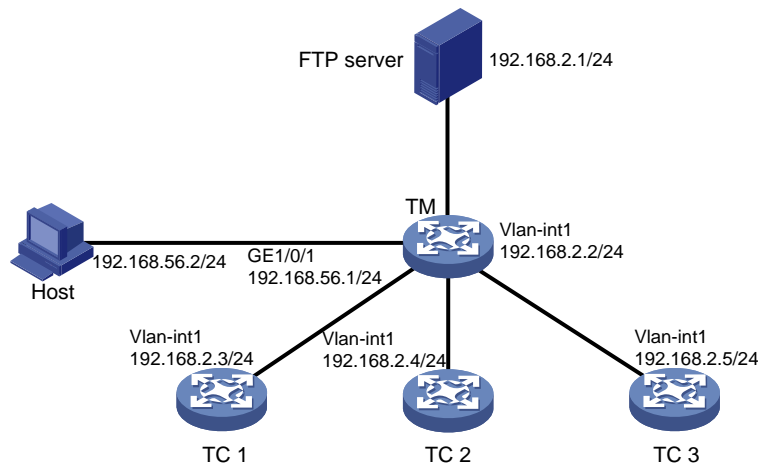
#### Network configuration

As shown in [Figure 3](#), member 1, member 2, and member 3 belong to the same device type: HPE FlexNetwork 5140 EI series. The IP address of the FTP server is 192.168.2.1. The FTP username is **admin** and the FTP password is **hello12345**.

Perform the following tasks to establish a SmartMC network and upgrade the configuration file on the members:

1. Configure the commander and members to automatically establish a SmartMC network.
2. Configure interface GigabitEthernet 1/0/1 as the outgoing interface for the SmartMC network.
3. Create a SmartMC group and add the members to the group.
4. Upgrade the configuration file on all members in the SmartMC group.
5. Save configuration file **startup.cfg** on the FTP server.

**Figure 5 Network diagram**



## Procedure

### 1. Configure TC 1:

#### # Configure VLAN-interface 1.

```

<TC1> system-view
[TC1] interface vlan-interface 1
[TC1-Vlan-interface1] ip address 192.168.2.3 24
[TC1-Vlan-interface1] quit

```

#### # Enable HTTP and HTTPS.

```

[TC1] ip http enable
[TC1] ip https enable

```

#### # Enable the Telnet service.

```

[TC1] telnet server enable

```

#### # Enable NETCONF over SOAP over HTTP.

```

[TC1] netconf soap http enable

```

#### # Enable LLDP globally.

```

[TC1] lldp global enable

```

#### # Create a user named **admin**.

```

[TC1] local-user admin

```

#### # Lower password complexity requirements. For more information about these commands, see password control commands in *Security Command Reference*.

```

[TC1-luser-manage-admin] password-control length 4
[TC1-luser-manage-admin] password-control composition type-number 1 type-length 1
[TC1-luser-manage-admin] undo password-control complexity user-name check

```

#### # Set the password to **admin**, add the **telnet**, **http**, and **https** service types, and authorize the user to use the **network-admin** user role.

```

[TC1-luser-manage-admin] password simple admin
[TC1-luser-manage-admin] service-type telnet http https
[TC1-luser-manage-admin] authorization-attribute user-role network-admin
[TC1-luser-manage-admin] quit

```

#### # Set scheme authentication for VTY user lines 0 to 63.

```

[TC1] line vty 0 63
[TC1-line-vty0-63] authentication-mode scheme

```

```

[TC1-line-vty0-63] quit
# Enable SmartMC and set the device role to tc.
[TC1] smartmc tc enable
2. Configure TC 2 and TC 3 in the same way TC 1 is configured. (Details not shown.)
3. Configure the TM:
# Configure GigabitEthernet 1/0/1.
<TM> system-view
[TM] interface gigabitethernet 1/0/1
[TM-GigabitEthernet1/0/1] port link-mode route
[TM-GigabitEthernet1/0/1] ip address 192.168.52.2 24
[TM-GigabitEthernet1/0/1] quit
# Configure VLAN-interface 1.
[TM] interface vlan-interface 1
[TM-Vlan-interface1] ip address 192.168.2.2 24
[TM-Vlan-interface1] quit
# Enable HTTP and HTTPS.
[TM] ip http enable
[TM] ip https enable
# Enable the Telnet service.
[TM] telnet server enable
# Enable NETCONF over SOAP over HTTP.
[TM] netconf soap http enable
# Enable LLDP globally.
[TM] lldp global enable
# Create a user. Set the username to admin and the password to hello12345, add the telnet,
http, and https service types, and authorize the user to use the network-admin user role.
[TM] local-user admin
[TM-luser-manage-admin] password simple hello12345
[TM-luser-manage-admin] service-type telnet http https
[TM-luser-manage-admin] authorization-attribute user-role network-admin
[TM-luser-manage-admin] quit
# Set scheme authentication for VTY user lines 0 to 63.
[TM] line vty 0 63
[TM-line-vty0-63] authentication-mode scheme
[TM-line-vty0-63] quit
# Enable SmartMC, set the device role to commander, and set the username to admin and the
password (plaintext) to hello12345.
[TM] smartmc tm username admin password simple hello12345 enable
# Specify GigabitEthernet 1/0/1 as the outgoing interface.
[TM] interface gigabitethernet 1/0/1
[TM-GigabitEthernet1/0/1] smartmc outbound
[TM-GigabitEthernet1/0/1] quit
# Set the FTP server IP address, username, and plaintext password to 192.168.2.1, admin,
and hello12345, respectively.
[TM] smartmc ftp-server 192.168.2.1 username admin password simple hello12345
# Create SmartMC group S1 and enter its view.
[TM] smartmc group S1

```

# Create an IP address match criterion to add all members in the specified network segment to SmartMC group **S1**.

```
[TM-smartmc-group-S1] match ip-address 192.168.2.0 24
```

# Specify the upgrade configuration file **startup.cfg** for SmartMC group **S1**.

```
[TM-smartmc-group-S1] startup-configuration startup.cfg
```

```
[TM-smartmc-group-S1] quit
```

# Upgrade the configuration file on all members in SmartMC group **S1**.

```
[TM] smartmc upgrade startup-configuration group S1 file startup.cfg
```

## Verifying the configuration

# Display brief information about all members after the SmartMC network is established.

```
[TM] display smartmc tc
```

| TCID | DeviceType        | Sysname | IpAddress   | MacAddress     | Status | Version         |
|------|-------------------|---------|-------------|----------------|--------|-----------------|
| 1    | 5140 24G 4SFP+ EI | TC1     | 192.168.2.3 | 201c-e7c3-0300 | Normal | COMWAREV700R001 |
| 2    | 5140 24G 4SFP+ EI | TC2     | 192.168.2.4 | 201c-e7c3-0301 | Normal | COMWAREV700R001 |
| 3    | 5140 24G 4SFP+ EI | TC3     | 192.168.2.5 | 201c-e7c3-0302 | Normal | COMWAREV700R001 |

# Display the configuration file upgrade status on the members.

```
<TM> display smartmc upgrade status
```

| ID | IpAddress   | MacAddress     | Status   | UpdateTime  | UpdateFile  |
|----|-------------|----------------|----------|-------------|-------------|
| 1  | 192.168.2.3 | 201c-e7c3-0300 | Finished | Immediately | startup.cfg |
| 2  | 192.168.2.4 | 201c-e7c3-0301 | Finished | Immediately | startup.cfg |
| 3  | 192.168.2.5 | 201c-e7c3-0302 | Finished | Immediately | startup.cfg |

## Command reference

### boot-loader file

Use **boot-loader file** to specify the upgrade startup software files for a SmartMC group.

Use **undo boot-loader** to restore the default.

### Syntax

```
boot-loader file { ipe-filename | boot boot-filename system system-filename }
```

```
undo boot-loader
```

### Default

No upgrade startup software files are specified for a SmartMC group.

### Views

SmartMC group view

### Predefined user roles

network-admin

### Parameters

*ipe-filename*: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

**boot** *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

**system** *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

## Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

## Examples

```
# Specify IPE software file device.ipe for SmartMC group testgroup.
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup] boot-loader file device.ipe
```

## Related commands

```
smartmc group
smartmc upgrade boot-loader
```

## create batch-file

Use **create batch-file** to create a batch file.

### Syntax

```
create batch-file batch-file-name
```

### Default

No batch files exist.

### Views

User view

### Predefined user roles

network-admin

### Parameters

*batch-file-name*: Specifies the name of the batch file, a case-insensitive string of 1 to 255 characters. If you do not specify a file extension when specifying a file name, the default extension **.cmdset** is used.

## Usage guidelines

After executing this command, you will enter the batch edit mode. In this mode, each command occupies a line. When you finish editing all command lines, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

## Examples

```
# Create a batch file named test.cmdset, and enter the command lines for specifying the device name as Sysname and enabling Telnet.
<Sysname> create batch-file test.cmdset
Begin to edit batch commands, and quit with the character '%'.
system-view
sysname Sysname
telnet server enable%
<Sysname>
```

## Related commands

```
display smartmc batch-file status
smartmc batch-file deploy
```

## display smartmc backup configuration status

Use `display smartmc backup configuration status` to display the backup status on members.

## Syntax

```
display smartmc backup configuration status
```

## Views

Any view

## Predefined user roles

network-admin

## Usage guidelines

This command displays the status of the ongoing backup task or the most recent backup task if the member is not performing backup.

## Examples

# Display the backup status on members.

```
<Sysname> display smartmc backup configuration status
```

| ID | IpAddress     | MacAddress     | Status   | Time                |
|----|---------------|----------------|----------|---------------------|
| 1  | 192.168.56.30 | 08d2-38ff-0300 | Finished | 2017-04-05 11:30:35 |
| 2  | 192.168.56.40 | 62d2-c21c-0400 | Finished | 2017-04-05 11:30:40 |

**Table 2 Command output**

| Field      | Description                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID         | ID of the member.                                                                                                                                                                                                                                                                                                                                                                                                        |
| IpAddress  | IP address of the member.                                                                                                                                                                                                                                                                                                                                                                                                |
| MacAddress | MAC address of the member.                                                                                                                                                                                                                                                                                                                                                                                               |
| Status     | Backup status: <ul style="list-style-type: none"><li>• <b>Waiting</b>—The member is waiting for configuration backup.</li><li>• <b>Processing</b>—The member is backing up the configuration.</li><li>• <b>Finished</b>—The member has finished backing up the configuration.</li><li>• <b>Timeout</b>—Configuration backup times out.</li><li>• <b>Failed</b>—The member failed to back up the configuration.</li></ul> |
| Time       | Time when the member finished backing up the configuration. If the member has not finished backing up the configuration, this field displays a hyphen (-).                                                                                                                                                                                                                                                               |

## Related commands

```
smartmc backup configuration
smartmc backup configuration interval
smartmc backup configuration max-number
```

## display smartmc batch-file status

Use **display smartmc batch-file status** to display the batch file deployment result.

### Syntax

```
display smartmc batch-file status [ ap | last number | phone ]
```

### Views

Any view

### Predefined user roles

network-admin

### Parameters

**ap**: Displays the result of the most recent batch file deployment for ports connected to APs.

**last number**: Specifies a batch file deployment (performed by using the **smartmc batch-file deploy** command) by its number counting from the most recent batch file deployment. The value range for the *number* argument is 1 to 5.

**phone**: Displays the result of the most recent batch file deployment for ports connected to IP phones.

### Usage guidelines

If you do not specify any parameters, this command displays the result of the most recent batch file deployment performed by using the **smartmc batch-file deploy** command.

### Examples

# Display the result of the most recent batch file deployment. In this example, the batch file contains the **display smartmc configuration** command.

```
<Sysname> display smartmc batch-file status last 1
```

```
TC ID 1
```

```
Device MAC : 8a73-60c3-0200
```

```
Start Time : 2018-12-24 14:55:39
```

```
End Time : 2018-12-24 14:55:43
```

```
Result :
```

```
<Sysname>display smartmc configuration
```

```
Device role : TC
```

```
TM IP : 192.168.22.103
```

```
TM MAC : 8a73-4faa-0100
```

```
TM sysname : Sysname
```

```
<Sysname>
```

```
TC ID 2
```

```
Device MAC : 8a73-6b31-0300
```

```
Start Time : 2018-12-24 14:55:43
```

```
End Time : 2018-12-24 14:55:48
```

```
Result :
```

```
<Sysname>display smartmc configuration
```

```
Device role : TC
```

```
TM IP : 192.168.22.103
```



```

TM MAC                : 8a73-4faa-0100
TM sysname            : Sysname
<Sysname>

```

**Table 3 Command output**

Field	Description
TC ID	ID of the member.
Device MAC	MAC address of the member.
Start Time	Batch file deployment start time.
End Time	Batch file deployment end time.
Result	Batch file deployment result in details.

## Related commands

```

create batch-file
smartmc batch-file apply
smartmc batch-file deploy

```

## display smartmc configuration

Use **display smartmc configuration** to display the SmartMC configuration.

## Syntax

```
display smartmc configuration
```

## Views

Any view

## Predefined user roles

network-admin

## Examples

# Display the SmartMC configuration on the commander.

```
<Sysname> display smartmc configuration
```

```
Device role                : TM
```

```
File server:
```

```
  Type: FTP
```

```
  IP address: 192.168.22.103
```

```
  Username: admin
```

```
  Port: 21
```

```
  VPN instance: N/A
```

```
  Directory: /FTP
```

```
Topology-refresh interval  : 60(s)
```

```
Backup startup-configuration interval : N/A
```

```
Sync backup number        : 5
```

```
Device status              : Lack
```

Some configurations are absent on the TM, such as Telnet or LLDP configuration.

# Display the commander information on a member.

```
<Sysname> display smartmc configuration
Device role       : TC
TM IP             : 192.168.22.103
TM MAC           : 8288-468d-0100
TM sysname       : Sysname
```

**Table 4 Command output**

Field	Description
Device role	Role of the device.
File server	File server configuration.
Type	File server type. If no file server is specified, this field displays <b>N/A</b> .
IP address	File server IP address. If no file server is specified, this field displays <b>N/A</b> .
Username	File server username. If no file server is specified, this field displays <b>N/A</b> .
Port	File server port. If no file server is specified, this field displays <b>N/A</b> .
VPN instance	VPN instance to which the file server belongs. If no file server is specified, this field displays <b>N/A</b> .
Directory	Storage directory of files on the file server. If no file server is specified, this field displays <b>N/A</b> .
Topology-refresh interval	Topology refresh interval, in seconds.
Backup startup-configuration interval	Automatic configuration file backup interval, in hours. If no interval is set, this field displays <b>N/A</b> .
Sync backup number	Number of members that can perform configuration backup at the same time.
Device status	Commander status: <ul style="list-style-type: none"> <li>• <b>Normal</b>.</li> <li>• <b>Lack</b>—Lack of configuration, such as NETCONF, Telnet, local user, and LLDP.</li> </ul>
TM IP	IP address of the commander. If the member failed to obtain the commander IP address, this field displays <b>N/A</b> .
TM MAC	MAC address of the commander. If the member failed to obtain the commander MAC address, this field displays <b>N/A</b> .
TM sysname	Name of the commander. If the member failed to obtain the commander name, this field displays <b>N/A</b> .
Some configurations are absent on the TM, such as XXX.	This field is available only when the <b>Device status</b> field displays <b>Lack</b> . Lack of configuration will affect SmartMC functions. Please follow the prompt to complete the configuration.

## Related commands

```
smartmc backup configuration interval
smartmc backup configuration max-number
smartmc enable
smartmc { ftp-server | sftp-server }
smartmc topology-refresh interval
```

## display smartmc device-link

Use **display smartmc device-link** to display connections between devices in the SmartMC network.

### Syntax

```
display smartmc device-link
```

### Views

Any view

### Predefined user roles

network-admin

### Examples

# Display connections between devices in the SmartMC network.

```
<Sysname> display smartmc device-link
```

```
(TM IP)[192.168.56.20]
```

ID	Hop	LocalPort	LocalIP	PeerPort	PeerIP
0	0	GigabitEthernet1/0/2	192.168.56.20	GigabitEthernet1/0/1	192.168.56.30
1	1	GigabitEthernet1/0/1	192.168.56.30	GigabitEthernet1/0/2	192.168.56.20
1	2	GigabitEthernet1/0/2	192.168.56.30	GigabitEthernet1/0/1	192.168.56.40
2	3	GigabitEthernet1/0/1	192.168.56.40	GigabitEthernet1/0/2	192.168.56.30

**Table 5 Command output**

Field	Description
TM IP	IP address of the commander.
ID	ID of the commander or member.
Hop	Number of hops between the commander and member.
LocalPort	Local port.
LocalIP	IP address of the local device.
PeerPort	Peer port.
PeerIP	IP address of the peer port.

### Related commands

```
smartmc topology-refresh
```

```
smartmc topology-refresh interval
```

## display smartmc group

Use **display smartmc group** to display SmartMC group information.

### Syntax

```
display smartmc group [ group-name ] [ verbose ]
```

### Views

Any view

### Predefined user roles

network-admin

## Parameters

*group-name*: Specifies a SmartMC group by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this argument, the command displays information about all SmartMC groups.

**verbose**: Displays detailed SmartMC group information. If you do not specify this keyword, the command displays brief SmartMC group information.

## Examples

# Display detailed SmartMC group information.

```
<Sysname> display smartmc group verbose
```

```
Group name           : test
```

```
TC count             : 3
```

```
Boot-loader file     :
```

```
Startup-configuration file :
```

```
Rule:
```

```
Match Device-type 5140 24G 4SFP+ EI
```

TCID	DeviceType	Sysname	IpAddress	MacAddress	Status	Version
1	5140 24G 4SFP+ EI	S1	192.168.56.103	0e74-e2fb-0400	Normal	COMWAREV700R001
2	5140 24G 4SFP+ EI	S2	192.168.56.102	0e74-ea13-0500	Normal	COMWAREV700R001
3	5140 24G 4SFP+ EI	S3	192.168.56.104	0e74-db54-0300	Normal	COMWAREV700R001

**Table 6 Command output**

Field	Description
GroupName	Name of the SmartMC group.
TC count	Number of members in the SmartMC group.
Boot-loader file	Names of the upgrade startup software files for upgrading the SmartMC group. If no upgrade startup software files are specified, this field displays null.
Startup-configuration file	Name of the configuration file for upgrading the SmartMC group. If no configuration file is specified, this field displays null.
Rule	Match criteria of the SmartMC group.
Match	Match type and its value. The match types include the following: <ul style="list-style-type: none"><li>• <b>Device-type</b>—Matches members by device type.</li><li>• <b>IP-address</b>—Matches members by IP address.</li><li>• <b>MAC-address</b>—Matches members by MAC address.</li></ul>
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Version	Software version of the member.
Status	Operating status of the member: <ul style="list-style-type: none"><li>• <b>Offline</b>—The member is offline.</li><li>• <b>Normal</b>—The member is online.</li></ul>

## Related commands

**match**

`smartmc group`

## display smartmc replace status

Use `display smartmc replace status` to display faulty member replacement status.

### Syntax

`display smartmc replace status`

### Views

Any view

### Predefined user roles

network-admin

### Examples

```
# Display faulty member replacement status.
<Sysname> display smartmc replace status
Faulty ID      : 2
Faulty MAC     : 94e2-cdcb-0600
Replacement ID : 3
Replacement MAC: 2443-5f8c-0200
Mode           : Manual
Status         : Successful
Start time     : 2017-03-21 15:01:31
End time       : 2017-03-21 15:01:40
```

**Table 7 Command output**

Field	Description
Faulty ID	ID of the faulty member.
Faulty MAC	MAC address of the faulty member.
Replacement ID	ID of the new member.
Replacement MAC	MAC address of the new member.
Mode	Replacement method, which can be <b>Manual</b> or <b>Auto</b> .
Status	Replacement status: <ul style="list-style-type: none"><li>• <b>Successful.</b></li><li>• <b>Failed.</b></li><li>• <b>Replacing.</b></li><li>• <b>Timeout.</b></li></ul>
Start time	Replacement start time
End time	Replacement end time.

### Related commands

`smartmc auto-replace enable`

`smartmc replace`

## display smartmc resource-monitor

Use `display smartmc resource-monitor` to display resource monitoring information.

## Syntax

```
display smartmc resource-monitor [ cpu | memory | temperature ] * [ tc  
tc-id | tm ]
```

## Views

Any view

## Predefined user roles

network-admin

## Parameters

**cpu**: Displays CPU usage.

**memory**: Displays memory usage.

**temperature**: Displays temperature information.

**tc tc-id**: Specify a member by its ID in the range of 1 to 255.

**tm**: Specify the commander.

## Usage guidelines

This command displays CPU usage, memory usage, and temperature information of the commander and members on the commander. For packet dropping information, log in to the Web interface of the commander and access the **SmartMC > Intelligent O&M > Resource monitoring** page.

If you do not specify a resource type, this command displays the resource monitoring information of all types.

If you do not specify a member or the commander, this command displays the resource monitoring information for the commander and all members.

## Examples

# Display the resource monitoring information for member 1.

```
<Sysname> display smartmc resource-monitor tc 1
```

```
TC 1
```

```
Collection time : 2017-07-25 18:02:30
```

```
Slot 1:
```

```
CPU 0 CPU usage: 1%
```

```
Memory usage   : 587076/903332
```

```
Temperature    : 30
```

**Table 8 Command output**

Field	Description
Collection time	Time when the resource monitoring information was collected.

## Related commands

```
smartmc resource-monitor
```

## display smartmc resource-monitor configuration

Use **display smartmc resource-monitor configuration** to display resource monitoring configuration.

## Syntax

```
display smartmc resource-monitor configuration
```

## Views

Any view

## Predefined user roles

network-admin

## Usage guidelines

This command displays CPU usage, memory usage, and temperature monitoring configuration of the commander. You can view the status of packet dropping monitoring by using the **display current-configuration | include smartmc** command.

## Examples

# Display resource monitoring configuration.

```
<Sysname> display smartmc resource-monitor configuration
```

ID	MacAddress	CPU	Memory	Temperature
1	1234-2222-3333	Y	N	N
2	1234-2222-3334	Y	N	N
3	1234-2222-3335	Y	N	N

**Table 9 Command output**

Field	Description
ID	Device ID.
MacAddress	MAC address of the device.
CPU	CPU usage monitoring status: <ul style="list-style-type: none"><li>• <b>Y</b>—CPU usage monitoring is enabled.</li><li>• <b>N</b>—CPU usage monitoring is disabled.</li><li>• —The device does not support CPU usage monitoring.</li></ul>
Memory	Memory usage monitoring status: <ul style="list-style-type: none"><li>• <b>Y</b>—Memory usage monitoring is enabled.</li><li>• <b>N</b>—Memory usage monitoring is disabled.</li><li>• —The device does not support memory usage monitoring.</li></ul>
Temperature	Temperature monitoring status: <ul style="list-style-type: none"><li>• <b>Y</b>—Temperature monitoring is enabled.</li><li>• <b>N</b>—Temperature monitoring is disabled.</li><li>• —The device does not support temperature monitoring.</li></ul>

## Related commands

**smartmc resource-monitor**

## display smartmc tc

Use **display smartmc tc** to display member information.

## Syntax

```
display smartmc tc [ tc-id ] [ verbose ]
```

## Views

Any view

## Predefined user roles

network-admin

## Parameters

*tc-id*: Specifies a member by its ID in the range of 1 to 255. If you do not specify a member, this command displays information about all members.

**verbose**: Displays detailed member information. If you do not specify this keyword, the command displays brief member information.

## Examples

# Display brief information about all members.

```
<Sysname> display smartmc tc
```

TCID	DeviceType	Sysname	IpAddress	MacAddress	Status	Version
1	5140 24G 4SFP+ EI	S1	192.168.22.104	201c-e7c3-0300	Normal	COMWAREV700R001

**Table 10 Command output**

Field	Description
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Operating status of the member: <ul style="list-style-type: none"><li>• <b>Normal</b>—The member is operating correctly.</li><li>• <b>Offline</b>—The member is offline.</li></ul>
Version	Software version of the member.

# Display detailed information about all members.

```
<Sysname> display smartmc tc verbose
```

```
TC ID                : 1
Adding method        : Manual
Sysname              : S1
Model                : 5140 24G 4SFP+ EI
Device type          : 5140-EI
SYSOID               : 1.3.6.1.4.1.25506
MAC address          : 0e74-e2fb-0400
IP address            : 192.168.56.103
Boot image           :
Boot image version    :
System image          :
System image version  :
Current-configuration file :
Uptime                : 2 days, 3 hours, 4 minutes
System CPU usage      : 0%
System memory usage   : 0%
Status                : Offline
Boot-loader file      :
Startup-configuration file :
```



**Table 11 Command output**

Field	Description
TC ID	ID of the member.
Adding method	Method through which the member is added to the SmartMC network: <ul style="list-style-type: none"> <li>Manual.</li> <li>Auto.</li> </ul>
Sysname	Device name of the member.
Model	Device model of the member.
Device type	Device type of the member.
SYSOID	SYSOID of the member.
MAC address	MAC address of the member.
IP address	IP address of the member.
Boot image	Boot image file that the member runs.
Boot image version	Version of the boot image file.
System image	System image file that the member runs.
System image version	Version of the system image file.
Current-configuration file	Current startup configuration file used by the member.
Uptime	Operation duration of the member.
System CPU usage	CPU usage on the member.
System memory usage	Memory usage on the member.
Status	Operating status of the member: <ul style="list-style-type: none"> <li><b>Normal</b>—The member is operating correctly.</li> <li><b>Offline</b>—The member is offline.</li> </ul>
Boot-loader file	Upgrade startup software files.
Startup-configuration file	Upgrade configuration file.

## display smartmc tc log buffer

Use **display smartmc tc log buffer** to display log information in the log buffer on a member.

### Syntax

```
display smartmc tc tc-id log buffer [ module module-name [ mnemonic mnemonic-value ] ]
```

### Views

Any view

### Predefined user roles

network-admin

### Parameters

*tc-id*: Specifies a member by its ID in the range of 1 to 255.

**module** *module-name*: Specifies a module by its name, a case-insensitive string of 1 to 8 characters. To display module names, use the **info-center source** command (see information center commands in *Network Management and Monitoring Command Reference*).

**mnemonic** *mnemonic-value*: Specifies a mnemonic, a case-insensitive string of 1 to 32 characters.

## Examples

# Display the log information for the SHELL module with the SHELL\_CMD mnemonic for member 1.

```
<Sysname> display smartmc tc 1 log buffer module SHELL mnemonic SHELL_CMD
```

```
Time      : 2017-07-15 13:51:46
```

```
Level     : Informational
```

```
Module    : SHELL
```

```
Mnemonic  : SHELL_CMD
```

```
Content   : -Line=con0-IPAddr=**-User=**; Command is qu
```

```
Time      : 2017-07-15 13:51:39
```

```
Level     : Informational
```

```
Module    : SHELL
```

```
Mnemonic  : SHELL_CMD
```

```
Content   : -Line=con0-IPAddr=**-User=**; Command is local-user admin
```

**Table 12 Command output**

Field	Description
Time	Time when the log was generated.
Level	Log level.

## display smartmc tc log restart

Use **display smartmc tc log restart** to display the restart log information for a member.

### Syntax

```
display smartmc tc tc-id log restart
```

### Views

Any view

### Predefined user roles

network-admin

### Parameters

*tc-id*: Specifies a member by its ID in the range of 1 to 255.

### Usage guidelines

In addition to saving the logs generated by modules to the log buffer, a member sends restart logs to the commander. The commander creates a restart log buffer for each member to store their restart logs.

The commander stores a maximum of 10 restart logs for each member. The most recent restart log overwrites the oldest one when there are more than 10 restart logs for a member.

You can also use the **display smartmc tc *tc-id* log buffer module SYSLOG mnemonic SYSLOG\_RESTART** command to display the restart log information.

## Examples

```
# Display the restart log information for member 1.
<Sysname> display smartmc tc 1 log restart
Time      : 2017-07-15 13:51:46
Level     : Informational
Module    : SYSLOG
Mnemonic  : SYSLOG_RESTART
Content   : System restarted -- HPE Comware Software.
```

**Table 13 Command output**

Field	Description
Time	Time when the log was generated.
Level	Log level.

## Related commands

```
display smartmc tc log buffer
```

## display smartmc upgrade status

Use `display smartmc upgrade status` to display member upgrade status.

## Syntax

```
display smartmc upgrade status
```

## Views

Any view

## Predefined user roles

network-admin

## Examples

```
# Display member upgrade status.
<Sysname> display smartmc upgrade status
ID      IpAddress      MacAddress      Status      UpdateTime      UpdateFile
1       192.168.56.1      82dd-a434-0200  Finished    Immediately      bootloader.ipe
2       192.168.56.103   5caf-2e5f-0100  Finished    Immediately      bootloader.ipe
```

**Table 14 Command output**

Field	Description
ID	ID of the member.
MacAddress	MAC address of the member.
IpAddress	IP address of the member.
Status	Upgrade status: <ul style="list-style-type: none"><li>• <b>Waiting</b>—The member is waiting for downloading the upgrade file.</li><li>• <b>Download-failed</b>—The member failed to download the upgrade file.</li><li>• <b>Download-finished</b>—The member has downloaded the upgrade file.</li><li>• <b>Downloading</b>—The member is downloading the upgrade file.</li><li>• <b>Updating</b>—The member is upgrading.</li><li>• <b>Finished</b>—The member has finished upgrading.</li></ul>

Field	Description
	<ul style="list-style-type: none"> <li><b>Failed</b>—The member failed to upgrade.</li> <li><b>Unknown</b>—The upgrade status of the member is unknown.</li> </ul>
Updated File	Name of the upgrade file.
UpdateTime	Upgrade time: <ul style="list-style-type: none"> <li><b>Immediately</b>—Upgrade at once.</li> <li><b>Delay(m)</b>—Upgrade after the specified delay.</li> <li><b>Time(HH:MM)</b>—Upgrade at the specified time.</li> </ul>

## Related commands

`smartmc upgrade group`

`smartmc upgrade tc`

## display smartmc vlan

Use `display smartmc vlan` to display VLAN creation results for members.

## Syntax

`display smartmc vlan`

## Views

Any view

## Predefined user roles

network-admin

## Examples

# Display VLAN creation results.

<Sysname> `display smartmc vlan`

ID	IpAddress	MacAddress	Vlan	Status
1	192.168.22.222	703d-15ad-cd02	2	Success
2	192.168.22.3	24ff-2264-0100	2	Success
3	192.168.22.4	24ff-2f74-0200	2	Success
4	192.168.22.223	487a-dac8-29ba	2	Success

**Table 15 Command output**

Field	Description
ID	Member ID.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Vlan	VLAN created for the member.
Status	VLAN creation status: <ul style="list-style-type: none"> <li><b>Processing</b>—The VLAN is being created.</li> <li><b>Success</b>—The VLAN has been created successfully.</li> <li><b>Failure. The port xxx is not an access port</b>—The VLAN fails to be created, because ports connected to non-SmartMC devices are not access ports.</li> <li><b>Failure. xxx not exist</b>—The VLAN fails to be created, because all access ports are connected to SmartMC devices.</li> </ul>

## Related commands

**smartmc vlan**

## match

Use **match** to set a match criterion to add all matching members to a SmartMC group.

Use **undo match** to delete a match criterion.

## Syntax

```
match { device-type device-type | ip-address ip-address { ip-mask-length  
| ip-mask } | mac-address mac-address mac-mask-length }
```

```
undo match { device-type device-type | ip-address ip-address  
{ ip-mask-length | ip-mask } | mac-address mac-address mac-mask-length }
```

## Default

No match criterion is set.

## Views

SmartMC group view

## Predefined user roles

network-admin

## Parameters

**device-type** *device-type*: Sets a device type match criterion.

**ip-address** *ip-address* { *ip-mask-length* | *ip-mask* }: Sets an IP address match criterion. The *ip-address* argument specifies an IP address in dotted decimal notation. The *ip-mask* argument specifies the subnet mask in dotted decimal notation. The *ip-mask-length* argument specifies the subnet mask length in the range of 1 to 32.

**mac-address** *mac-address* *mac-mask-length*: Sets a MAC address match criterion. The *mac-address* argument specifies a MAC address in the format of *H-H-H*. The *mac-mask-length* argument specifies the mask length in the range of 1 to 48.

## Examples

# Create a SmartMC group named **a** and add members in subnet 192.168.1.0/24 to the group.

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

```
[Sysname] smartmc group a
```

```
[Sysname-smartmc-group-a] match ip-address 192.168.1.0 24
```

## Related commands

**smartmc group**

**display smartmc group**

## smartmc auto-link-aggregation enable

Use **smartmc auto-link-aggregation enable** to enable automatic Ethernet link aggregation.

Use **undo smartmc auto-link-aggregation enable** to disable automatic Ethernet link aggregation.

## Syntax

```
smartmc auto-link-aggregation enable
```

```
undo smartmc auto-link-aggregation enable
```

## Default

Automatic Ethernet link aggregation is disabled.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

Automatic Ethernet link aggregation is performed only between member devices.

Enabling or disabling automatic Ethernet link aggregation might cause network flapping, and the members might go offline for a short period of time.

## Examples

```
# Enable automatic Ethernet link aggregation.  
<Sysname> system-view  
[Sysname] smartmc auto-link-aggregation enable
```

## smartmc auto-replace enable

Use **smartmc auto-replace enable** to enable the automatic faulty member replacement feature.

Use **undo smartmc auto-replace enable** to disable the automatic faulty member replacement feature.

## Syntax

```
smartmc auto-replace enable  
undo smartmc auto-replace enable
```

## Default

The automatic faulty member replacement feature is disabled.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

To perform an automatic fault replacement, first enable this feature on the commander, and then perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

## Examples

```
# Enable the automatic faulty member replacement feature.  
<Sysname> system-view  
[Sysname] smartmc auto-replace enable
```

## Related commands

**smartmc replace**

## smartmc backup configuration

Use **smartmc backup configuration** to manually back up the configuration file on members.

### Syntax

```
smartmc backup configuration { group group-name-list | tc [ tc-id-list ] }
```

### Views

System view

### Predefined user roles

network-admin

### Parameters

**group** *group-name-list*: Specifies a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

**tc** *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a device or a range of devices in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 0 to 255, with 0 representing the commander and 1 to 255 representing members. If you do not specify the commander or any members, all devices will perform configuration backup.

### Usage guidelines

After you execute this command, the members immediately save the running configuration to the next-startup configuration files and upload the configuration files to the file server.

The backup configuration files are named in the format of *bridge MAC address\_backup.cfg*.

### Examples

# Back up the configuration file on member 1, member 2, member 3, and member 4.

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

```
[Sysname] smartmc backup configuration tc 1 to 4
```

# Back up the configuration file on all members in SmartMC groups **test1**, **test2**, and **test3**.

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

```
[Sysname] smartmc backup configuration group test1 test2 test3
```

## Related commands

**display smartmc configuration**

**smartmc backup configuration interval**

## smartmc backup configuration max-number

Use **smartmc backup configuration max-number** to set the maximum number of members that can perform automatic configuration backup at the same time.

Use **undo smartmc backup configuration max-number** to restore the default.

### Syntax

```
smartmc backup configuration max-number max-number
```

```
undo smartmc backup configuration max-number
```

## Default

A maximum of five members can perform automatic configuration backup at the same time.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*max-number*: Specifies the maximum number of members that can perform automatic configuration backup at the same time, in the range of 2 to 20.

## Usage guidelines

The maximum number of members that can perform automatic configuration at the same time is limited by the performance of the file server. If automatic configuration backup fails, set the maximum number of members to a smaller value.

## Examples

```
# Specify that a maximum of 10 members can perform automatic configuration backup at the same time.
<Sysname> system-view
[Sysname] smartmc backup configuration max-number 10
```

## Related commands

```
display smartmc configuration
smartmc backup configuration
smartmc backup configuration interval
```

## smartmc backup configuration interval

Use **smartmc backup configuration interval** to enable the automatic configuration file backup feature and set the automatic backup interval.

Use **undo smartmc backup configuration interval** to restore the default.

## Syntax

```
smartmc backup configuration interval interval
undo smartmc backup configuration interval
```

## Default

The automatic configuration file backup feature is disabled.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*interval*: Specifies the automatic configuration file backup interval in the range of 1 to 720 hours.

## Usage guidelines

This command enables the commander and members to back up their configuration files by saving the running configuration to the files and then uploading them to the file server. When you execute



this command, the commander and members immediately perform a backup. After that, they back up the configuration files at the specified interval. The backup configuration files are named in the format of *bridge MAC address\_backup.cfg*.

## Examples

# Enable the automatic configuration file backup feature and set the backup interval to 24 hours.

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

```
[Sysname] smartmc backup configuration interval 24
```

## Related commands

**display smartmc configuration**

**smartmc backup configuration**

## smartmc batch-file apply

Use **smartmc batch-file apply** to specify a batch file to deploy to ports connecting APs or IP phones.

Use **undo smartmc batch-file apply** to remove a batch file specified for ports connecting APs or IP phones.

## Syntax

```
smartmc batch-file batch-file-name apply { ap | phone }
```

```
undo smartmc batch-file apply { ap | phone }
```

## Default

No batch file is specified for ports connecting APs or IP phones.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*batch-file-name*: Specifies a batch file by its name, a case-insensitive string of 1 to 255 characters.

**ap**: Specifies ports connecting APs.

**phone**: Specifies ports connecting IP phones.

## Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration.

When the commander first detects the association of an AP or IP phone on a port through LLDP, it deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

If the AP or IP phone disconnects from the port, the configurations on the port remain. When a new device comes online from the port, configurations used by the port depend on the new device type.

- If the new device is an AP or IP phone and has the same type as the disconnected device, the configurations on the port remain unchanged.
- If the new device is an AP or IP phone but has a different type as the disconnected device, the commander deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

- If the new device is neither an AP nor an IP phone, the configurations on the port remain unchanged.

To disable the commander from deploying a batch file to ports, remove the specified batch file or execute the **undo smartmc batch-file-apply enable** command to disable batch file deployment.

## Examples

# Specify batch file **ap.cmdset** for ports connecting APs or IP phones.

```
<Sysname> system-view
[Sysname] smartmc batch-file ap.cmdset apply ap
```

## Related commands

```
create batch-file
smartmc batch-file-apply enable
```

## smartmc batch-file deploy

Use **smartmc batch-file deploy** to deploy bulk command lines to a list of members or SmartMC groups.

## Syntax

```
smartmc batch-file batch-file-name deploy { group group-name-list | tc
tc-id-list }
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

*batch-file-name*: Specifies the name of a batch file, a case-insensitive string of 1 to 255 characters.

**group** *group-name-list*: Specifies a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

**tc** *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

## Examples

# Deploy batch file **startup.cmdset** to SmartMC group **testgroup**.

```
<Sysname> system-view
[Sysname] smartmc batch-file startup.cmdset deploy group testgroup
```

## Related commands

```
create batch-file
display smartmc batch-file status
```

## smartmc batch-file-apply enable

Use **smartmc batch-file-apply enable** to enable batch file deployment.

Use **undo smartmc batch-file-apply enable** to disable batch file deployment.

## Syntax

```
smartmc batch-file-apply enable
undo smartmc batch-file-apply enable
```

## Default

Batch file deployment is enabled.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration. To disable the commander from deploying a batch file to ports, remove the specified batch file or disable batch file deployment.

## Examples

```
# Disable batch file deployment.
<Sysname> system-view
[Sysname] undo smartmc batch-file-apply enable
```

## Related commands

```
smartmc batch-file apply
```

## smartmc enable

Use **smartmc enable** to enable SmartMC and set the device role.

Use **undo smartmc enable** to disable SmartMC.

## Syntax

```
smartmc { tc | tm username username password { cipher | simple } string }
enable
undo smartmc enable
```

## Default

SmartMC is disabled.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**tc**: Enables SmartMC and sets the device role to member.

**tm**: Enables SmartMC and sets the device role to commander.

**username** *username*: Specifies a username for the local user, a case-sensitive string of 1 to 55 characters.

**password**: Specifies a password for the local user.

**cipher**: Specifies a password in encrypted form.

**simple**: Specifies a password in plaintext 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 1 to 117 characters.

## Usage guidelines

A SmartMC network must have one and only one commander.

To enable SmartMC, execute this command on both the commander and members. To configure the other SmartMC features, execute associated commands only on the commander.

If you change the role of the commander to member or disable SmartMC on the commander, all SmartMC settings in its running configuration will be cleared.

SmartMC fails to be enabled if ACL resources are insufficient. If ACL resources are insufficient, use the **undo acl** command to delete unnecessary ACLs and then enable SmartMC. You can execute the **display acl** command to view ACL configuration and match statistics. For more information about ACLs, see *ACL and QoS Configuration Guide*.

SmartMC fails to be enabled if ports 80 and 443 have been used.

If you execute this command multiple times, the most recent configuration takes effect. You can execute the command to change the device role or the password.

## Examples

# Enable SmartMC and set the device role to member.

```
<Sysname> system-view  
[Sysname] smartmc tc enable
```

## smartmc { ftp-server | sftp-server }

Use **smartmc { ftp-server | sftp-server }** to configure the file server information.

Use **undo smartmc { ftp-server | sftp-server }** to delete the file server information.

## Syntax

```
smartmc { ftp-server | sftp-server } { ipv4-address | ipv6 ipv6-address }  
[ port port ] [ vpn-instance vpn-instance-name ] [ directory directory ]  
username username password { cipher | simple } string  
undo smartmc { ftp-server | sftp-server }
```

## Default

No file server information is configured.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**ftp-server**: Specifies an FTP server.

**sftp-server**: Specifies an SFTP server.

**ipv4-address**: Specifies the IPv4 address of the file server.

**ipv6 ipv6-address**: Specifies the IPv6 address of the file server.

**port** *port*: Specifies the port number of the file server, in the range of 1 to 65535. The default port for an FTP server and an SFTP server is 21 and 22, respectively.

**vpn-instance** *vpn-instance-name*: Specifies the name of the MPLS L3VPN instance to which the file server belongs, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command considers that the file server is in the public network.

**directory** *directory*: Specifies the working directory of the file server, a case-insensitive string. By default, the root directory is used.

**username** *username*: Specifies the file server username, a case-sensitive string of 1 to 55 characters.

**password**: Specifies the file server password.

**cipher**: Specifies a password in encrypted form.

**simple**: Specifies a password in plaintext 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 1 to 117 characters.

## Usage guidelines

You can specify only one file server. If you execute this command multiple times, the most recent configuration takes effect.

## Examples

# Set the file server type to FTP, and specify the server IP address, username, and password as 192.168.22.19, **admin**, and **hello12345**, respectively.

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

```
[Sysname] smartmc ftp-server 192.168.22.19 username admin password simple hello12345
```

## Related commands

**display smartmc configuration**

## smartmc group

Use **smartmc group** to create a SmartMC group and enter its view, or enter the view of an existing SmartMC group.

Use **undo smartmc group** to delete a SmartMC group.

## Syntax

**smartmc group** *group-name*

**undo smartmc group** *group-name*

## Default

No SmartMC groups exist.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*group-name*: Specifies the name of the SmartMC group, a case-sensitive string of 1 to 31 characters.

## Usage guidelines

When you perform the following operations, you can specify a SmartMC group to apply the operations to all members in the group:

- Startup software upgrade.
- Configuration file upgrade.
- Configuration deployment.

## Examples

```
# Create SmartMC group testgroup.  
<Sysname> system-view  
[Sysname] smartmc group testgroup  
[Sysname-smartmc-group-testgroup]
```

## Related commands

**match**

## smartmc outbound

Use **smartmc outbound** to configure an outgoing interface for the SmartMC network.

Use **undo smartmc outbound** to restore the default.

## Syntax

```
smartmc outbound  
undo smartmc outbound
```

## Default

No interface is used as an outgoing interface, and the SmartMC network cannot communicate with outside networks.

## Views

VLAN interface view

## Predefined user roles

network-admin

## Usage guidelines

VLAN interface 1 cannot be used as an outgoing interface, because the SmartMC network is established in VLAN 1.

## Examples

```
# Configure GigabitEthernet 1/0/1 as an outgoing interface for the SmartMC network.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] smartmc outbound
```

## smartmc resource-monitor

Use **smartmc resource-monitor** to enable resource monitoring.

Use **undo smartmc resource-monitor** to disable resource monitoring.

## Syntax

```
smartmc resource-monitor [ cpu | memory | packet-drop | temperature ] *  
[ group group-name-list | tc { tc-id-list | mac-address mac-address } | tm ]  
  
undo smartmc resource-monitor [ cpu | memory | packet-drop | temperature ]  
* [ group group-name-list | tc { tc-id-list | mac-address mac-address } | tm ]
```

## Default

Resource monitoring is disabled.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**cpu**: Enables CPU usage monitoring.

**memory**: Enables memory usage monitoring.

**packet-drop**: Enables packet dropping monitoring.

**temperature**: Enables temperature monitoring.

**group group-name-list**: Specifies the SmartMC groups to monitor. You can specify a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

**tc**: Specifies the members to monitor.

**tc-id-list**: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

**mac-address mac-address**: Specifies a member by its MAC address in the format of H-H-H.

**tm**: Enables resource monitoring on the commander.

## Usage guidelines

Packet dropping monitoring monitors packet dropping on members and on interfaces.

If you do not specify a resource type, this command enables resource monitoring for all resource types.

If you do not specify a device to monitor (member or the commander), this command enables resource monitoring on the commander and all members.

## Examples

```
# Enable resource monitoring for all resource types on member 1 through member 3.
```

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

```
[Sysname] smartmc resource-monitor tc 1 to 3
```

## Related commands

```
display smartmc resource-monitor
```

```
smartmc resource-monitor interval
```

```
smartmc resource-monitor max-age
```

## smartmc resource-monitor interval

Use **smartmc resource-monitor interval** to set the interval for the commander to obtain resource monitoring information.

Use **undo smartmc resource-monitor interval** to restore the default.

### Syntax

```
smartmc resource-monitor interval interval  
undo smartmc resource-monitor interval
```

### Default

The interval for the commander to obtain resource monitoring information is 1 minute.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*interval*: Specifies the interval for the commander to obtain resource monitoring information, in the range of 1 to 60 minutes.

### Usage guidelines

For packet dropping monitoring, the specified interval applies only to obtaining of member packet dropping information. Because of the great amount of interface information, the commander obtains interface packet dropping information from members only when Web displaying is requested.

### Examples

```
# Set the interval for the commander to obtain resource monitoring information to 5 minutes.  
<Sysname> system-view  
[Sysname] smartmc resource-monitor interval 5
```

### Related commands

```
display smartmc resource-monitor  
smartmc resource-monitor
```

## smartmc resource-monitor max-age

Use **smartmc resource-monitor max-age** to set the aging time for resource monitoring information.

Use **undo smartmc resource-monitor max-age** to restore the default.

### Syntax

```
smartmc resource-monitor max-age max-age  
undo smartmc resource-monitor max-age
```

### Default

The aging time for resource monitoring information is 24 hours.

### Views

System view



## Predefined user roles

network-admin

## Parameters

*max-age*: Specifies the aging time for resource monitoring information, in the range of 1 to 168 hours.

## Usage guidelines

For packet dropping monitoring, the specified aging time applies only to member packet dropping information. Each member saves its interface packet dropping information for as long as 30 days.

To view interface packet dropping information, log in to the Web interface of the commander and access the **SmartMC > Intelligent O&M > Resource monitoring** page. You can view information in the past 1 hour, 1 day, or 30 days.

## Examples

```
# Set the aging time for resource monitoring information to 1 hour.
```

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

```
[Sysname] smartmc resource-monitor max-age 1
```

## Related commands

```
display smartmc resource-monitor
```

```
smartmc resource-monitor
```

## smartmc replace

Use **smartmc replace** to manually replace a faulty member.

## Syntax

```
smartmc replace tc tc-id1 faulty-tc tc-id2
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**tc** *tc-id1*: Specifies the ID of the new member, in the range of 1 to 255.

**faulty-tc** *tc-id2*: Specifies the ID of the faulty member, in the range of 1 to 255.

## Usage guidelines

Before you execute this command, perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

## Examples

```
# Replace faulty member 5 with new member 10.
```

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

```
[Sysname] smartmc replace tc 10 faulty-tc 5
```

## Related commands

```
display smartmc replace status
smartmc auto-replace enable
```

## smartmc tc boot-loader

Use **smartmc tc boot-loader** to specify the upgrade startup software files for a member.

Use **undo smartmc tc boot-loader** to remove the configuration.

## Syntax

```
smartmc tc tc-id boot-loader { ipe-filename | boot boot-filename system
system-filename }
undo smartmc tc tc-id boot-loader
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**tc** *tc-id*: Specifies a member by its ID in the range of 1 to 255.

*ipe-filename*: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

**boot** *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

**system** *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

## Examples

# Specify upgrade boot image **boot.bin** and upgrade system image **system.bin** for member 1.

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

```
[Sysname] smartmc tc 1 boot-loader boot boot.bin system system.bin
```

## Related commands

```
display smartmc tc
```

## smartmc tc device-type

Use **smartmc tc device-type** to define a member type on the commander.

Use **undo smartmc tc device-type** to delete a member type.

## Syntax

```
smartmc tc sysoid sysoid device-type device-type
undo smartmc tc sysoid sysoid device-type device-type
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**sysoid** *sysoid*: Specifies the SYSOID of a member.

**device-type** *device-type*: Specifies a member type.

## Usage guidelines

A device type can correspond to multiple device models. You can identify different device models with different SYSOIDs by specifying a SYSOID for each device model. The commander identifies member types by SYSOID.

The system predefines the device types for some device models based on SYSOIDs. For device models without predefined device types, you must define their member types by SYSOID manually. If you do not do so, the commander cannot identify the types of such devices.

You cannot modify the predefined device types.

Before defining a device type for a member, you can use the **display smartmc tc** command to determine whether the member has a predefined one.

- If the member has been predefined with one device type, the **DeviceType** field displays the actual predefined device type.
- If the member does not have a predefined device type, the **DeviceType** field displays **unknown**.

To obtain the SYSOID of a member, use the **display smartmc tc verbose** command.

## Examples

# Define a member type by specifying the SYSOID as 1.3.6.1.4.1.25506.1.1588 and the member type as SW.

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

```
[Sysname] smartmc tc sysoid 1.3.6.1.4.1.25506.1.1588 device-type SW
```

## smartmc tc password

Use **smartmc tc password** to modify the password for the default user (admin) on members.

Use **undo smartmc tc password** to restore the default.

## Syntax

```
smartmc tc password [ cipher ] string
```

```
undo smartmc tc password
```

## Default

The password for the default user on members is **admin**.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**cipher**: Specifies a password in encrypted form. If you do not specify this keyword, the command creates 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.

## Usage guidelines

During SmartMC network establishment, the commander establishes NETCONF sessions to members and adds them to the network. The default username and password on the members for NETCONF session establishment are **admin** and **admin**. To enhance security, you can perform this task to change the password for the default user **admin** of the members after the commander adds the members to the network.

If the default password cannot meet the password complexity requirements on members, you cannot execute the **undo smartmc tc password** command to restore the default.

Do not modify the password for members that are manually added to the SmartMC network. If you modify the password for a manually added member, you will not be able to manage that member from the commander.

## Examples

# Configure default user admin on members to use plaintext password **hello12345**.

```
<Sysname> system-view
[Sysname] smartmc tc password hello12345
```

## smartmc tc startup-configuration

Use **smartmc tc startup-configuration** to specify the upgrade configuration file for a member.

Use **undo smartmc tc startup-configuration** to remove the configuration.

## Syntax

```
smartmc tc tc-id startup-configuration cfg-filename
undo smartmc tc tc-id startup-configuration
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**tc** *tc-id*: Specifies a member by its ID in the range of 1 to 255.

*cfg-filename*: Specifies a configuration file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.cfg** extension.

## Examples

# Specify upgrade configuration file **startup.cfg** for member 1.

```
<Sysname> system-view
[Sysname] smartmc tc 1 startup-configuration startup.cfg
```

## Related commands

```
display smartmc tc
```

## smartmc topology-refresh

Use **smartmc topology-refresh** to manually refresh the network topology.

## Syntax

```
smartmc topology-refresh
```

## Views

Any view

## Predefined user roles

network-admin

## Usage guidelines

To display topology changes, use this command to manually refresh the topology.

## Examples

```
# Manually refresh the network topology.  
<Sysname> smartmc topology-refresh
```

## Related commands

**display smartmc device-link**

## smartmc topology-refresh interval

Use **smartmc topology-refresh interval** to set the automatic network topology refresh interval.

Use **undo smartmc topology-refresh interval** to restore the default.

## Syntax

```
smartmc topology-refresh interval interval  
undo smartmc topology-refresh interval
```

## Default

The automatic network topology refresh interval is 60 seconds.

## Views

System view

## Predefined user roles

network-admin

## Parameters

*interval*: Specifies the automatic network topology refresh interval in the range of 60 to 300 seconds.

## Examples

```
# Set the automatic network topology refresh interval to 100 seconds.  
<Sysname> system-view  
[Sysname] smartmc topology-refresh interval 100
```

## Related commands

**display smartmc device-link**

## smartmc topology-save

Use **smartmc topology-save** to save the current network topology.

## Syntax

```
smartmc topology-save
```

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

This task allows you to save the current network topology to the **topology.dba** file in the flash memory. After the commander reboots, it uses the **topology.dba** file to restore the network topology.

## Examples

```
# Save the current network topology
<Sysname> system-view
[Sysname] smartmc topology-save
```

## Related commands

**display smartmc device-link**

## smartmc upgrade boot-loader

Use **smartmc upgrade boot-loader** to upgrade the startup software on a list of members or SmartMC groups.

Use **undo smartmc upgrade** delete the startup software upgrade task.

## Syntax

```
smartmc upgrade boot-loader { group | tc } list [ delay minutes | time
time ]

smartmc upgrade boot-loader { group | tc } { list { boot boot-filename
system system-filename | file ipe-filename } }<1-40> [ delay delay-time
| time time ]

undo smartmc upgrade
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**group**: Specifies the SmartMC groups to be upgraded.

**tc**: Specifies the members to be upgraded.

**list**: Specifies a space-separated list of up to 10 member items or SmartMC group items.

- **SmartMC group**—Each item specifies a SmartMC group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

**boot** *boot-filename*: Specifies a boot image by its name.

**system** *system-filename*: Specifies a system image by its name.

**file** *ipe-filename*: Specifies an IPE file by its name, a case-insensitive string of 5 to 45 characters.

**delay** *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

**time** *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

## Usage guidelines

### ⚠ CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

To use this command to upgrade the startup software on members without specifying the upgrade files, you must first perform one of the following tasks:

- Execute the **smartmc tc boot-loader** command to specify the upgrade files for members.
- Execute the **boot-loader** command to specify the upgrade files for a SmartMC group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or SmartMC group immediately upgrades the startup software and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

## Examples

# Upgrade startup software images **boot.bin** and **sys.bin** on all members in SmartMC groups **test1** and **test2**.

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

```
[Sysname] smartmc upgrade boot-loader group test1 test2 boot boot.bin system sys.bin
```

## Related commands

**boot-loader**

**startup-configuration**

## smartmc upgrade startup-configuration

Use **smartmc upgrade startup-configuration** to upgrade the configuration file on a list of members or on all members in SmartMC groups.

Use **undo smartmc upgrade** delete the configuration file upgrade task.

## Syntax

```
smartmc upgrade startup-configuration { group | tc } list [ delay minutes  
| time time ]
```

```
smartmc upgrade startup-configuration group { list file  
cfg-filename }&<1-40> [ delay delay-time | time time ]
```

```
smartmc upgrade startup-configuration tc { list cfg-filename }&<1-40>  
[ delay delay-time | time time ]
```

```
undo smartmc upgrade
```

## Views

System view

## Predefined user roles

network-admin

## Parameters

**group**: Specifies the SmartMC groups to be upgraded.

**tc**: Specifies the members to be upgraded.

**list**: Specifies a space-separated list of up to 10 member items or SmartMC group items.

- **SmartMC group**—Each item specifies a SmartMC group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

**file** *cfg-filename*: Specifies a configuration file by its name.

**delay** *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

**time** *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

## Usage guidelines



### CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

To use this command to upgrade the configuration file on members without specifying the upgrade file, you must first perform one of the following tasks:

- Execute the **smartmc tc startup-configuration** command to specify the upgrade file for members.
- Execute the **startup-configuration** command to specify the upgrade file for a SmartMC group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or SmartMC group immediately upgrades the configuration file and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

## Examples

# Upgrade configuration file **startup.cfg** on all members in SmartMC groups **test1** and **test2**.

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

```
[Sysname] smartmc upgrade boot-loader group test1 test2 file startup.cfg
```

## Related commands

**boot-loader**

**startup-configuration**

## smartmc vlan

Use **smartmc vlan** to create a VLAN for members.

## Syntax

```
smartmc vlan vlan-id { group group-name-list | tc tc-id-list }
```



## Views

System view

## Predefined user roles

network-admin

## Parameters

*vlan-id*: Specifies the VLAN ID in the range of 1 to 4094.

**group** *group-name-list*: Specifies the SmartMC groups for which the VLAN is created. You can specify a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

**tc** *tc-id-list*: Specifies the members for which the VLAN is created. You can specify a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

## Usage guidelines

Execute this command when the network topology is stable. As a best practice, use the **smartmc topology-refresh** command to refresh the network topology before executing this command.

After you execute this command, all access ports on members except the following access ports are assigned to the VLAN:

- Access ports connecting to the commander.
- Access ports connecting to other members.
- Access ports connecting to offline devices. Remove offline devices before configuring this command.

If the VLAN is successfully created but some access ports of a member cannot be assigned to the VLAN, the VLAN memberships of the member is restored to the state before the VLAN is created.

The failure to assign an access port of a member to the created VLAN does not affect the VLAN assignment for other members.

After command execution, you can use the **display smartmc vlan** command to examine the VLAN creation result.

## Examples

# Create a VLAN for member 1 and member 2.

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

```
[Sysname] smartmc vlan 2 tc 1 to 2
```

As a best practice, execute the **display smartmc vlan** command to verify that the VLAN has been created successfully.

## startup-configuration

Use **startup-configuration** to specify an upgrade configuration file for a SmartMC group .

Use **undo startup-configuration** to restore the default.

## Syntax

**startup-configuration** *cfgfile*

**undo startup-configuration**

## Default

No upgrade configuration file is specified for the SmartMC group.

## Views

SmartMC group view

## Predefined user roles

network-admin

## Parameters

*cfgfile*: Specifies a configuration file by its name, a string of 5 to 45 characters. The file name must include the **.cfg** extension.

## Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

## Examples

```
# Specify configuration file startup.cfg for SmartMC group testgroup.
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup] startup-configuration startup.cfg
```

# New feature: Configuring interface alarm functions

## Configuring interface alarm functions

### About this task

With the interface alarm functions enabled, when the number of error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

### Restrictions and guidelines

You can configure the error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

An interface that is shut down because of error packet alarms cannot automatically recover. To bring up the interface, execute the **undo shutdown** command on the interface.

To ensure that error packet statistics are accurate, make sure the value for the **interval interval** option is greater than 7.

### Enabling interface alarm functions

1. Enter system view.  
**system-view**
2. Enable alarm functions for the interface monitoring module.  
**snmp-agent trap enable ifmonitor [ crc-error ]**  
By default, all alarm functions are enabled for interfaces.

### Configuring CRC error packet parameters

4. Enter system view.  
**system-view**
3. Configure global CRC error packet alarm parameters.  
**ifmonitor crc-error slot slot-number high-threshold high-value low-threshold low-value interval interval [ shutdown ]**  
By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packets.
4. Enter Ethernet interface view.  
**interface interface-type interface-number**
5. Configure CRC error packet alarm parameters for the interface.  
**port ifmonitor crc-error high-threshold high-value low-threshold low-value interval interval [ shutdown ]**  
By default, an interface uses the global CRC error packet alarm parameters.

# Command reference

## ifmonitor crc-error

Use **ifmonitor crc-error** to configure global CRC error packet alarm parameters.

Use **undo ifmonitor crc-error** to restore the default.

### Syntax

```
ifmonitor crc-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown ]  
undo ifmonitor crc-error slot slot-number
```

### Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packet alarms.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**high-threshold** *high-value*: Specifies the upper threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

**low-threshold** *low-value*: Specifies the lower threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

**interval** *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

**shutdown**: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

**slot** *slot-number*: Specifies an IRF member device by its member ID.

### Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

## Examples

```
# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms.
```

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

```
[Sysname] ifmonitor crc-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

## Related commands

```
snmp-agent trap enable ifmonitor
```

## port ifmonitor crc-error

Use **port ifmonitor crc-error** to configure CRC error packet alarm parameters for an interface.

Use **undo port ifmonitor crc-error** to restore the default.

## Syntax

```
port ifmonitor crc-error high-threshold high-value low-threshold low-value interval interval [ shutdown ]
```

```
undo port ifmonitor crc-error
```

## Default

An interface uses the global CRC error packet alarm parameters.

## Views

Ethernet interface view

## Predefined user roles

network-admin

## Parameters

**high-threshold** *high-value*: Specifies the upper threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

**low-threshold** *low-value*: Specifies the lower threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

**interval** *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

**shutdown**: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

## Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.

- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

## Examples

# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor crc-error high-threshold 5000
low-threshold 400 interval 6
```

## Related commands

**snmp-agent trap enable ifmonitor**

## snmp-agent trap enable ifmonitor

Use **snmp-agent trap enable ifmonitor** to enable interface alarm functions.

Use **undo snmp-agent trap enable ifmonitor** to disable interface alarm functions.

## Syntax

```
snmp-agent trap enable ifmonitor [ crc-error ]
undo snmp-agent trap enable ifmonitor [ crc-error ]
```

## Default

Interface alarm functions are enabled.

## Views

System view

## Predefined user roles

network-admin

## Parameters

**crc-error**: Enables the CRC error packet alarm function for interfaces.

## Examples

# Enable the CRC error packet alarm function for interfaces.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ifmonitor crc-error
```

# New feature: Configuring Option 60 for DHCP requests

## Configuring Option 60 for DHCP requests

### About this task

Option 60 acts as a vendor class identifier (VCI). You can configure a DHCP client to send a request with Option 60 for the DHCP server to make class-based IP address assignment. When the DHCP server receives a request with Option 60 from a client, the server identifies the user class of the client. Then, the server assigns the client an IP address from the IP range specified for the user class.

By default, Option 60 contains the vendor name and the product name. To define this option for DHCP requests, perform this task.

## Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type* *interface-number*
3. Configure Option 60 for DHCP requests.  
**dhcp client class-id** { **ascii** *ascii-string* | **hex** *hex-string* }  
By default, Option 60 contains the vendor name and the product name.

## Command reference

### dhcp client class-id

Use **dhcp client class-id** to configure Option 60.

Use **undo dhcp client class-id** to restore the default.

#### Syntax

```
dhcp client class-id { ascii ascii-string | hex hex-string }  
undo dhcp client class-id
```

#### Default

Option 60 contains the vendor name and the product name.

#### Views

Interface view

#### Predefined user roles

network-admin

#### Parameters

**ascii** *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the content in Option 60.

**hex** *hex-string*: Specifies a case-sensitive hexadecimal string of 4 to 64 characters as the value in Option 60.

#### Usage guidelines

Option 60 acts as a vendor class identifier (VCI). You can configure a DHCP client to send a request with Option 60 for the DHCP server to make class-based IP address assignment. When the DHCP server receives a request with Option 60 from a client, the server identifies the user class of the client. Then, the server assigns the client an IP address from the IP range specified for the user class.

By default, Option 60 contains the vendor name and the product name. To customize this option, use this command.

#### Examples

# Configure FFFFFFFF as the content of Option 60 on VLAN-interface 10.

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] dhcp client class-id hex FFFFFFFF
```

# New feature: Configuring the type of port ID TLVs advertised by LLDP

## Configuring the type of port ID TLVs advertised by LLDP

### About this task

An HPE device determines whether it has an MED neighbor based on received LLDPDUs. If the LLDPDUs contain LLDP-MED TLVs, the device determines that it has an MED neighbor. By default, the device advertises port ID TLVs that contain interface MAC addresses out of interfaces that have MED neighbors. If no MED neighbor exists on an interface, the device advertises port ID TLVs that contain interface names through the interface.

This task enables an HPE device to advertise only port ID TLVs that contain interface names. The media devices from some vendors can obtain interface information from HPE devices only through LLDP. For the media devices to obtain interface names, you must configure HPE devices to generate port ID TLVs based on interface names.

### Restrictions and guidelines

Perform this task only when LLDP neighbors must obtain interface names from LLDPDUs. Do not perform this task in any other scenarios.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

### Configuring the type of port ID TLVs advertised by LLDP globally

1. Enter system view.

**system-view**

1. Configure the type of port ID TLVs advertised by LLDP.

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] global  
tlv-config basic-tlv port-id type-id
```

By default, an interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

### Configuring the type of port ID TLVs advertised by LLDP on an interface

1. Enter system view.

**system-view**

2. Enter interface view.

```
interface interface-type interface-number
```

2. Configure the type of port ID TLVs advertised by LLDP.

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-config  
basic-tlv port-id type-id
```

By default, an interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.



## Command reference

### lldp global tlv-config basic-tlv port-id

Use **lldp global tlv-config basic-tlv port-id** to set the type of port ID TLVs advertised by LLDP globally.

Use **undo lldp global tlv-config basic-tlv port-id** to restore the default.

#### Syntax

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] global tlv-config  
basic-tlv port-id type-id
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] global  
tlv-config basic-tlv port-id
```

#### Default

An interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

#### Views

System view

#### Predefined user roles

network-admin

#### Parameters

**agent**: Specifies an LLDP agent type. If you do not specify an agent type, the command sets the port ID TLV type for nearest bridge agents.

**nearest-customer**: Specifies nearest customer bridge agents.

**nearest-nontpmr**: Specifies nearest non-TPMR bridge agents.

**type-id**: Specifies a port ID TLV type. The available value is 5, which represents that port ID TLVs contain interface names.

#### Usage guidelines

This command enables the device to advertise only port ID TLVs that contain interface names. Execute this command if LLDP neighbors must obtain interface names from LLDPDUs.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

#### Examples

```
# Enable the device to advertise port ID TLVs that contain interface names.
```

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

```
[Sysname] lldp global tlv-config basic-tlv port-id 5
```

#### Related commands

```
lldp tlv-config basic-tlv port-id
```

### lldp tlv-config basic-tlv port-id

Use **lldp tlv-config basic-tlv port-id** to set the type of port ID TLVs advertised by LLDP on an interface.

Use **undo lldp tlv-config basic-tlv port-id** to restore the default.

## Syntax

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-config basic-tlv
port-id type-id

undo lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-config
basic-tlv port-id
```

## Default

An interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

## Views

Layer 2 Ethernet interface view  
Management Ethernet interface view  
Layer 2 aggregate interface view

## Predefined user roles

network-admin

## Parameters

**agent**: Specifies an LLDP agent type. If you do not specify an agent type, the command sets the port ID TLV type for nearest bridge agents.

**nearest-customer**: Specifies nearest customer bridge agents.

**nearest-nontpmr**: Specifies nearest non-TPMR bridge agents.

**type-id**: Specifies a port ID TLV type. The available value is 5, which represents that port ID TLVs contain interface names.

## Usage guidelines

This command enables an interface to advertise only port ID TLVs that contain interface names. Execute this command if LLDP neighbors must obtain interface names from LLDPDUs.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

## Examples

```
# Enable GigabitEthernet 1/0/1 to advertise port ID TLVs that contain interface names.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-config basic-tlv port-id 5
```

## Related commands

```
lldp global tlv-config basic-tlv port-id
```

# New feature: Enabling displaying LLDP local information about all interfaces

## Enabling displaying LLDP local information about all interfaces

### About this task

This task enables the **display lldp local-information** command to display LLDP local information about all interfaces.

By default, the **display lldp local-information** command displays information about physically up interfaces. The media devices from some vendors can obtain interface information from HPE devices only through LLDP. For the media devices to obtain all interface information, enable the **display lldp local-information** command to display LLDP local information about all interfaces.

## Restrictions and guidelines

Perform this task only when LLDP neighbors must obtain all interface information from the device through LLDP.

## Procedure

1. Enter system view.

```
system-view
```

1. Enable displaying LLDP local information about all interfaces.

```
lldp local-information all-interface
```

By default, the **display lldp local-information** command displays information about physically up interfaces.

## Command reference

### lldp local-information all-interface

Use **lldp local-information all-interface** to enable displaying LLDP local information about all interfaces.

Use **undo lldp local-information all-interface** to disable displaying LLDP local information about interfaces not in physically up state.

## Syntax

```
lldp local-information all-interface
```

```
undo lldp local-information all-interface
```

## Default

The **display lldp local-information** command displays information about physically up interfaces.

## Views

System view

## Predefined user roles

network-admin

## Usage guidelines

This command enables the **display lldp local-information** command to display LLDP local information about all interfaces.

By default, the **display lldp local-information** command displays information about physically up interfaces. The media devices from some vendors can obtain interface information from HPE devices only through LLDP. For the media devices to obtain all interface information, enable the **display lldp local-information** command to display LLDP local information about all interfaces.

## Examples

```
# Enable displaying LLDP local information about all interfaces.
```

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

```
[Sysname] lldp local-information all-interface
```

## Related commands

```
display lldp local-information
```

# New feature: PoE forced power supply

## Enabling PoE forced power supply

### About this task

Before supplying power to a PD, the device performs a detection of the PD. It supplies power to the PD only after the PD passes the detection. If the PD fails the detection but the power provided by the device meets the PD specifications, you can perform this task to enable forced power supply to the PD.

### Restrictions and guidelines

This feature enables the device to supply power to a PD directly without performing a detection of the PD. To avoid damaging the PD, make sure the power provided by the device meets the PD specifications before performing this task.

After enabling PoE forced power supply on a PI, the system reserves the maximum power for the PI even if no PD is attached to the PI or the PI is not enabled with PoE. For the maximum power that a PI can deliver, execute the **display poe pse pse-id interface power** command. For the maximum power that the PSE can allocate, execute the **display poe pse** command.

### Procedure

1. Enter system view.  
**system-view**
  2. Enter PI view.  
**interface** *interface-type* *interface-number*
  3. Enable PoE forced power supply.  
**poe force-power**
- By default, PoE forced power supply is disabled.

## Command reference

### poe force-power

Use **poe force-power** to enable PoE forced power supply.

Use **undo poe force-power** to disable PoE forced power supply.

### Syntax

```
poe force-power  
undo poe force-power
```

### Default

PoE forced power supply is disabled.

### Views

PI view

## Predefined user roles

network-admin

## Usage guidelines

### CAUTION:

This command enables the device to supply power to a PD directly without performing a detection of the PD. To avoid damaging the PD, make sure the power provided by the device meets the PD specifications before executing this command.

Before supplying power to a PD, the device performs a detection of the PD. It supplies power to the PD only after the PD passes the detection. If the PD fails the detection but the power provided by the device meets the PD specifications, you can execute this command to enable forced power supply to the PD.

After enabling PoE forced power supply on a PI, the system reserves the maximum power for the PI even if no PD is attached to the PI or the PI is not enabled with PoE. For the maximum power that a PI can deliver, execute the **display poe pse pse-id interface power** command. For the maximum power that the PSE can allocate, execute the **display poe pse** command.

## Examples

# Enable PoE forced power supply.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe force-power
```

The PD might be damaged if the power provided by the device does not meet the PD power specifications. Continue? [Y/N]:y

## Command changes

### Modified command: display poe pse

#### Syntax

```
display poe pse
```

#### Views

Any view

#### Change description

Before modification: The output from the **display poe pse** command does not contain the **Max Allocable Power** field.

After modification: The **Max Allocable Power** field was added to the output from the **display poe pse** command. The value for the field is equal to the maximum power of the PSE minus the sum of the maximum powers of all PIs on which PoE forced power supply is enabled.

# New feature: Interval at which the SNMP module examines the system configuration for changes

## Setting the interval at which the SNMP module examines the system configuration for changes

### About this task

This task enables the SNMP module to examine the system configuration for changes at the specified interval and generate a trap and a log if any change is found.

### Procedure

1. Enter system view.  
**system-view**
2. Set the interval at which the SNMP module examines the system configuration for changes.  
**snmp-agent configuration-examine interval *interval***  
By default, the SNMP module examines the system configuration for changes at intervals of 600 seconds.

## Command reference

### snmp-agent configuration-examine interval

Use **snmp-agent configuration-examine interval** to set the interval at which the SNMP module examines the system configuration for changes.

Use **undo snmp-agent configuration-examine interval** to restore the default.

### Syntax

```
snmp-agent configuration-examine interval interval  
undo snmp-agent configuration-examine interval
```

### Default

By default, the SNMP module examines the system configuration for changes at intervals of 600 seconds.

### Views

System view

### Predefined user roles

network-admin

### Parameters

*interval*: Specifies the interval at which the SNMP module examines the system configuration for changes. The value is in the range of 1 to 86400, in seconds.

### Usage guidelines

This command enables the SNMP module to examine the system configuration for changes at the specified interval and generate a trap and a log if any change is found.

## Examples

```
# Set the interval at which the SNMP module examines the system configuration for changes to 600 seconds.
<sysname> system-view
[sysname] snmp-agent configuration-examine interval 600
```

## New feature: Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users

### Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users

#### About this task

#### ❗ IMPORTANT:

This feature must operate in conjunction with the IP source guard (IPSG) feature.

By default, the device generates a dynamic IPv4SG or IPv6SG binding entry for an 802.1X authenticated user after the user obtains a static or DHCP assigned IP address.

To allow only 802.1X users with DHCP assigned IP addresses to access the network, perform the following operations:

- Enable IPSG.
- Disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.
- Enable DHCP snooping. The device will generate IPv4SG or IPv6SG binding entries for the users based on DHCP snooping.

For more information about IPSG, see IP source guard in *Security Configuration Guide*.

#### Restrictions and guidelines

This feature takes effect only on 802.1X users that come online after the feature is enabled. If the IP address of an online 802.1X user changes, the device will update the dynamic IPv4SG or IPv6SG binding entry for the user.

Disabling this feature does not delete the existing dynamic IPv4SG or IPv6SG binding entries for online 802.1X users. If the IP address of an online 802.1X user changes after the feature is disabled, the device will delete the dynamic IPv4SG or IPv6SG binding entry for the user.

#### Procedure

1. Enter system view.  
**system-view**
2. Enter interface view.  
**interface** *interface-type* *interface-number*
3. Enable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

```
dot1x { ip-verify-source | ipv6-verify-source } enable
```

By default, generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users is enabled.

## dot1x { ip-verify-source | ipv6-verify-source } enable

Use **dot1x { ip-verify-source | ipv6-verify-source } enable** to enable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

Use **undo dot1x { ip-verify-source | ipv6-verify-source } enable** to disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

### Syntax

```
dot1x { ip-verify-source | ipv6-verify-source } enable
undo dot1x { ip-verify-source | ipv6-verify-source } enable
```

### Default

Generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users is enabled.

### Views

Layer 2 Ethernet interface view  
Layer 2 aggregate interface view

### Predefined user roles

network-admin  
mdc-admin

### Usage guidelines

---

#### ❗ IMPORTANT:

This feature must operate in conjunction with the IP source guard (IPSG) feature.

---

The **dot1x { ip-verify-source | ipv6-verify-source } enable** command takes effect only on 802.1X users that come online after the command is used. If the IP address of an online 802.1X user changes, the device will update the dynamic IPv4SG or IPv6SG binding entry for the user.

The **undo dot1x { ip-verify-source | ipv6-verify-source } enable** command does not delete the existing dynamic IPv4SG or IPv6SG binding entries for online 802.1X users. If the IP address of an online 802.1X user changes after the command is used, the device will delete the dynamic IPv4SG or IPv6SG binding entry for the user.

### Examples

# Disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x ip-verify-source enable
```

## New feature: Automated IPv6 underlay network deployment for VCF fabric

### About automated IPv6 underlay network deployment

As from this software version, the VCF fabric feature supports automated IPv6 underlay network deployment. The deployment procedure is the same as that of automated IPv4 underlay network deployment.



In an IPv6 VCF fabric, the controller collects the topology automatically. You do not need to specify a master spine node.

## Command reference

None.

## Modified feature: Setting the port status detection timer

### Feature change description

As from this release, the value range for the port status detection timer is changed to 0 to 3600 seconds.

The device starts a port status detection timer when a port is shut down by a protocol such as LLDP and loop detection. Once the timer expires, the device brings up the port so the port status reflects the port's physical status. For example, loop detection shuts down a looped interface to disable the interface from receiving or sending frames. The device automatically sets the interface to the forwarding state after the port status detection timer expires.

## Command changes

### Modified command: shutdown-interval

#### Syntax

```
shutdown-interval interval  
undo shutdown-interval
```

#### Views

System view

#### Change description

Before modification: The value range for the *interval* argument is 0 to 300.

After modification: The value range for the *interval* argument is 0 to 3600.

## Modified feature: 802.1X EAD assistant

### Feature change description

As from this version, you can use the **dot1x ead-assistant permit authentication-escape** command to enable support for 802.1X Auth-Fail and critical VLANs in 802.1X EAD assistant.

## Command changes

### New command: dot1x ead-assistant permit authentication-escape

Use **dot1x ead-assistant permit authentication-escape** to enable support for 802.1X Auth-Fail and critical VLANs in 802.1X EAD assistant.

Use `undo dot1x ead-assistant permit authentication-escape` to restore the default.

### Syntax

```
dot1x ead-assistant permit authentication-escape
undo dot1x ead-assistant permit authentication-escape
```

### Default

802.1X Auth-Fail and critical VLANs cannot take effect when 802.1X EAD assistant is enabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

This command enables the device to remove the EAD entries of users before it assigns the users to 802.1X Auth-Fail and critical VLANs.

### Examples

```
# Enable support for 802.1X Auth-Fail and critical VLANs in 802.1X EAD assistant.
<Sysname> system-view
[Sysname] dot1x ead-assistant permit authentication-escape
```

### Related commands

```
dot1x ead-assistant enable
```

## Modified feature: Displaying information about online 802.1X users

### Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the `display dot1x connection` command.

### Command changes

#### Modified command: display dot1x connection

### Syntax

```
display dot1x connection [ open ] [ interface interface-type
interface-number | slot slot-number | user-mac mac-address | user-name
name-string ]
```

### Views

Any view

### Change description

The **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display dot1x connection** command:

```
<Sysname> display dot1x connection
```

```
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```
User access state: Successful
```

```
Authentication domain: aaa
```

```
IPv4 address: 192.168.1.1
```

```
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
```

```
Authentication method: CHAP
```

```
Initial VLAN: 1
```

```
Authorization untagged VLAN: 6
```

```
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33  
                                35 37 40 to 100
```

```
Authorization VSI: N/A
```

```
Authorization ACL number/name: 3001
```

```
Authorization dynamic ACL name: N/A
```

```
Authorization user profile: N/A
```

```
Authorization CAR: N/A
```

```
Authorization URL: N/A
```

```
Termination action: Default
```

```
Session timeout period: 2 s
```

```
Online from: 2013/03/02 13:14:15
```

```
Online duration: 0h 2m 15s
```

## Modified feature: Displaying information about online MAC authentication users

### Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the **display mac-authentication connection** command.

### Command changes

#### 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 **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display mac-authentication connection** command:

```
<Sysname> display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: macusers
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 2 sec
Offline detection: 100 sec (server-assigned)
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s
```

## Modified feature: L2PT for CFD

### Feature change description

As from this version, the device supports enabling L2TP for CFD and configuring the destination multicast MAC address for tunneled packets of the specified protocol.

### Command changes

#### Modified command: l2protocol type tunnel-dmac

##### Old syntax

```
l2protocol type { cdp | dldp | dtp | eoam | gvrp | larp | lldp | mvrp |
pagp | pvst | stp | udld | vtp } tunnel-dmac mac-address
undo l2protocol type { cdp | dldp | dtp | eoam | gvrp | larp | lldp | mvrp |
pagp | pvst | stp | udld | vtp } tunnel-dmac
```

## New syntax

```
l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp |  
mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac mac-address  
  
undo l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp  
| mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac
```

## Views

System view

## Change description

Before modification: The **cfd** keyword is not supported.

After modification: The **cfd** keyword is supported.

## Modified command: l2protocol tunnel dot1q

## Old syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst |  
stp | udld | vtp } tunnel dot1q  
  
undo l2protocol { cdp | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp |  
pvst | stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld | vtp }  
tunnel dot1q  
  
undo l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q
```

## New syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp |  
pvst | stp | udld | vtp } tunnel dot1q  
  
undo l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp  
| pvst | stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q  
  
undo l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp  
| udld | vtp } tunnel dot1q
```

## Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

## Change description

Before modification: The **cfd** keyword is not supported.

After modification: The **cfd** keyword is supported.

## Modified command: display l2protocol statistics

### Syntax

```
display l2protocol statistics [ interface interface-type
interface-number ]
```

### Views

Any view

### Change description

Before modification: The device does not support displaying L2TP statistics for CFD protocol packets.

After modification: The device supports displaying L2TP statistics for CFD protocol packets.

# Display L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

```
<Sysname> display l2protocol statistics
```

L2PT statistics information on interface Bridge-Aggregation1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDP	0	3	0	0
EOAM	0	2	0	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	0	3	0	0
MVRP	0	0	0	0
PAGP	0	1	0	0
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0
CFD	0	0	0	0

L2PT statistics information on interface GigabitEthernet1/0/1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDP	2	3	3	0
EOAM	5	2	9	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	3	3	3	3
MVRP	0	0	0	0
PAGP	5	1	7	3
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0

CFD	0	0	0	0
-----	---	---	---	---

# Release 6330

This release has the following changes:

- [New feature: Enabling fast PoE for a PSE](#)
- [Modified feature: L2PT for CFD and DTP](#)
- [Modified feature: Displaying information about online 802.1X users](#)
- [Modified feature: Displaying information about online MAC authentication users](#)

## New feature: Enabling fast PoE for a PSE

### Enabling fast PoE for a PSE

#### About this task

This feature enables PIs on a PSE to supply power to PDs immediately after the PSE is powered on.

#### Restrictions and guidelines

You must re-configure this feature if you changed other PoE settings after configuring this feature.

#### Procedure

1. Enter system view.  
**system-view**
2. Enable fast PoE for a PSE.  
**poe fast-on enable pse** *pse-id*  
By default, fast PoE is disabled for a PSE.

## Command reference

### poe fast-on enable

Use **poe fast-on enable** to enable fast PoE for a PSE.

Use **undo poe fast-on enable** to disable fast PoE for a PSE.

#### Syntax

```
poe fast-on enable pse pse-id  
undo poe fast-on enable pse pse-id
```

#### Default

Fast PoE is disabled for a PSE.

#### Views

System view

#### Predefined user roles

network-admin

#### Parameters

**pse** *pse-id*: Specifies a PSE by its ID.



## Usage guidelines

Fast PoE enables PIs on a PSE to supply power to PDs immediately after the PSE is powered on.

You must re-configure this command if you changed other PoE settings after configuring this command.

## Examples

```
# Enable fast PoE for PSE 4.
<Sysname> system-view
[Sysname] poe fast-on enable pse 4
```

# Modified feature: L2PT for CFD and DTP

## Feature change description

As from this version, the device supports enabling L2TP for CFD and DTP and configuring the destination multicast MAC address for tunneled packets of the specified protocol.

## Command changes

### New command: l2protocol type tunnel-dmac

Use **l2protocol type tunnel-dmac** to set the destination multicast MAC address for tunneled packets of the specified protocol.

Use **undo l2protocol type tunnel-dmac** to restore the default.

### Syntax

```
l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp |
mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac mac-address

undo l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp
| mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac
```

### Default

The tunneled packets of all protocols use 010f-e200-0003 as the destination multicast MAC address.

### Views

System view

### Predefined user roles

network-admin

### Parameters

**cdp**: Specifies CDP.  
**cfd**: Specifies CFD.  
**dldp**: Specifies DLDP.  
**dtp**: Specifies DTP.  
**eoam**: Specifies EOAM.  
**gvrp**: Specifies GVRP.  
**lacp**: Specifies LACP.

**lldp**: Specifies LLDP.

**mvrp**: Specifies MVRP.

**pagp**: Specifies PAgP.

**pvst**: Specifies PVST.

**stp**: Specifies STP.

**udld**: Specifies UDLD.

**vtp**: Specifies VTP.

*mac-address*: Specifies a destination multicast MAC address for tunneled packets of the specified protocol, in the range of 0100-0000-0000 to 01ff-ffff-ffff.

## Usage guidelines

As a best practice, set different destination multicast MAC addresses on PEs connected to different customer networks. It prevents L2PT from sending packets of a customer network to another customer network.

The **l2protocol tunnel-dmac** command sets the destination multicast MAC address for tunneled packets of all protocols. This command sets the destination multicast MAC address for tunneled packets of the specified protocol. If both commands are executed, the **l2protocol type tunnel-dmac** command takes priority.

For tunneled packets to be recognized, set the same destination multicast MAC address for packets of the same protocol on PEs that are connected to the same customer network.

If you execute this command multiple times for a protocol, the most recent configuration takes effect.

## Examples

# Set the destination multicast MAC address to 0100-0ccd-cddc for tunneled packets of CFD.

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

```
[Sysname] l2protocol type cfd tunnel-dmac 0100-0ccd-cddc
```

## Modified command: l2protocol tunnel dot1q

### Old syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | dldp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst | stp |  
udld | vtp } tunnel dot1q
```

```
undo l2protocol { cdp | dldp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst |  
stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld | vtp }  
tunnel dot1q
```

```
undo l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q
```

### New syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp |  
pvst | stp | udld | vtp } tunnel dot1q
```

```
undo l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp  
| pvst | stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q  
  
undo l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp  
| udld | vtp } tunnel dot1q
```

## Views

layer 2 Ethernet interface view

layer 2 aggregate interface view

## Change description

Before modification: L2TP cannot be enabled for CFD or DTP.

After modification: L2TP can be enabled for CFD and DTP.

## Modified command: display l2protocol statistics

## Syntax

```
display l2protocol statistics [ interface interface-type  
interface-number ]
```

## Views

Any view

## Change description

Before modification: The device does not support displaying L2TP statistics for CFD or DTP protocol packets.

After modification: The device supports displaying L2TP statistics for CFD and DTP protocol packets.

# Display L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

```
<Sysname> display l2protocol statistics
```

L2PT statistics information on interface Bridge-Aggregation1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDP	0	3	0	0
EOAM	0	2	0	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	0	3	0	0
MVRP	0	0	0	0
PAGP	0	1	0	0
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0
CFD	0	0	0	0

L2PT statistics information on interface GigabitEthernet1/0/1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
----------	--------------	--------------	-----------	---------

CDP	0	0	0	0
DLDP	2	3	3	0
EOAM	5	2	9	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	3	3	3	3
MVRP	0	0	0	0
PAGP	5	1	7	3
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0
CFD	0	0	0	0

## Modified feature: Displaying information about online 802.1X users

### Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the **display dot1x connection** command.

### Command changes

#### Modified command: display dot1x connection

##### Syntax

```
display dot1x connection [ open ] [ interface interface-type
interface-number | slot slot-number | user-mac mac-address | user-name
name-string ]
```

##### Views

Any view

##### Change description

The **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display dot1x connection** command:

```
<Sysname> display dot1x connection
```

```
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```

User access state: Successful
Authentication domain: aaa
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100

Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s

```

## Modified feature: Displaying information about online MAC authentication users

### Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the **display mac-authentication connection** command.

### Command changes

#### 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 **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display mac-authentication connection** command:

```

<Sysname> display mac-authentication connection
Total connections: 1
Slot ID: 1

```

User MAC address: 0015-e9a6-7cfe  
Access interface: GigabitEthernet1/0/1  
Username: ias  
User access state: Successful  
Authentication domain: macusers  
IPv4 address: 192.168.1.1  
IPv6 address: 2000:0:0:0:1:2345:6789:abcd  
Initial VLAN: 1  
Authorization untagged VLAN: 100  
Authorization tagged VLAN: N/A  
Authorization VSI: N/A  
Authorization ACL number/name: 3001  
Authorization dynamic ACL name: N/A  
Authorization user profile: N/A  
Authorization CAR: N/A  
Authorization URL: N/A  
Termination action: Radius-request  
Session timeout period: 2 sec  
Offline detection: 100 sec (server-assigned)  
Online from: 2013/03/02 13:14:15  
Online duration: 0h 2m 15s