



**Hewlett Packard**  
Enterprise

# HPE 5120v3-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 .....	1
Upgrade restrictions and guidelines.....	3
Hardware feature updates .....	3
5120v3-CMW710-R6367 .....	3
5120v3-CMW710-R6352P02.....	3
Software feature and command updates .....	3
MIB updates .....	3
Operation changes .....	3
Operation changes in R6367 .....	3
Operation changes in R6352P02.....	3
Restrictions and cautions.....	4
Restrictions .....	4
Cautions .....	4
Open problems and workarounds .....	4
List of resolved problems.....	4
Resolved problems in R6367 .....	4
Resolved problems in R6352P02 .....	7
Support and other resources .....	7
Accessing Hewlett Packard Enterprise Support.....	7
Documents .....	7
Related documents .....	8
Documentation feedback .....	8
Appendix A Feature list.....	9
Hardware features.....	9
Software features.....	10
Appendix B Upgrading software .....	13
System software file types .....	13
System startup process.....	13
Upgrade methods.....	14
Preparing for the upgrade .....	15

Verifying device status .....	15
Setting up the upgrade environment .....	15
Upgrading from the CLI .....	16
Preparing for the upgrade .....	16
Downloading software images to the master switch .....	17
Upgrading from the Boot menu .....	21
Prerequisites .....	21
Accessing the Boot menu .....	22
Accessing the extended Boot menu .....	23
Upgrading Comware images from the Boot menu .....	24
Upgrading Boot ROM from the Boot menu .....	32
Managing files from the Boot menu .....	39
Handling software upgrade failures .....	42

# List of tables

Table 1 Version history .....	1
Table 2 Hardware and software compatibility matrix .....	1
Table 3 MIB updates .....	3
Table 4 5120v3 series hardware features.....	9
Table 5 Software features of the 5120v3 series .....	10
Table 6 Minimum free storage space requirements.....	21
Table 7 Shortcut keys .....	22
Table 8 Extended Boot ROM menu options.....	23
Table 9 EXTENDED ASSISTANT menu options .....	24
Table 10 TFTP parameter description .....	25
Table 11 FTP parameter description.....	26
Table 12 TFTP parameter description .....	33
Table 13 FTP parameter description.....	34

# Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version HPE 5120v3-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 5120v3-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 **Note①**.

### Version history

#### ! IMPORTANT:

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

**Table 1 Version history**

Version number	Last version	Release date	Release type	Remarks
5120v3-CMW710-R6367	5120v3-CMW710-R6352P02	2024-09-12	Release version	Fixed bugs
5120v3-CMW710-R6352P02	First release	2023-05-18	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	5120v3 Series
Hardware platform	HPE NW CW 5120v3 8G PoE+ 2 SFP Sw S0F79A
Memory	512M
Flash	256M

Item	Specifications
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	5120v3-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 5120v3

```
<HPE>display version
```

```
HPE Comware Software, Version 7.1.070, Release 6367 -----Note①
Copyright (c) 2010-2024 Hewlett Packard Enterprise Development LP
HPE NW CW 5120v3 8G PoE+ 2 SFP Sw uptime is 0 weeks, 0 days, 0 hours, 2 minutes
Last reboot reason : Cold reboot
```

```
Boot image: flash:/5120v3-cmw710-boot-r6367.bin
Boot image version: 7.1.070, Release 6367
Compiled Aug 08 2024 16:00:00
System image: flash:/5120v3-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
NW CW 5120v3 8G PoE+ 2 SFP Sw with 1 Processor
BOARD TYPE:      NW CW 5120v3 8G PoE+ 2 SFP Sw
DRAM:            512M bytes
FLASH:           256M bytes
PCB 1 Version:    VER.A
Bootrom Version:  158 -----Note②
CPLD 1 Version:   001
Release Version:  HPE NW CW 5120v3 8G PoE+ 2 SFP Sw S0F79A-6367
Patch Version :   None
Reboot Cause :    ColdReboot
[SubSlot 0] 8GE+2SFP
```

# 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

### 5120v3-CMW710-R6367

None.

### 5120v3-CMW710-R6352P02

First release.

## Software feature and command updates

For more information about the software feature and command update history, see *HPE 5120v3-CMW710-R6367 Release Notes (Software Feature Changes)*.

## MIB updates

Table 3 MIB updates

Item	MIB file	Module	Description
<b>5120v3-CMW710-R6367</b>			
New	None	None	None
Modified	None	None	None
<b>5120v3-CMW710-R6352P02</b>			
New	First release	First release	First release
Modified	First release	First release	First release

## Operation changes

### Operation changes in R6367

support ipv6 ready.

### Operation changes in R6352P02

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.

#### **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.

## Resolved problems in R6352P02

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 Networking Comware 5120v3 Switch Series Configuration Guides-R63xx
- HPE Networking Comware 5120v3 Switch Series Command References-R63xx
- HPE Networking Comware 5120v3 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 5120v3 series hardware features**

Item	NW CW 5120v3 8G PoE+ 2 SFP Sw
Dimensions (H x W x D)	43.6 x 330 x 230 mm (1.72 x12.99 x 9.06 in)
Weight	≤ 3 kg (6.61 lb)
Console port	1 x serial console port
10/100/1000B ASE-T autosensing Ethernet port	8
SFP port	2
Input voltage	Rated voltage: 100 VAC to 240 VAC @ 50 or 60 Hz Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz
Maximum PoE power per port	30 W
Total PoE power	125 W
Minimum power consumption	10W
Maximum power consumption	155W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943
Melting current of power module fuse	6.3 A/250 V
Cooling system	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

# Software features

**Table 5 Software features of the 5120v3 series**

Feature	5120v3 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>• 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> </ul>

	<ul style="list-style-type: none"> <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 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:

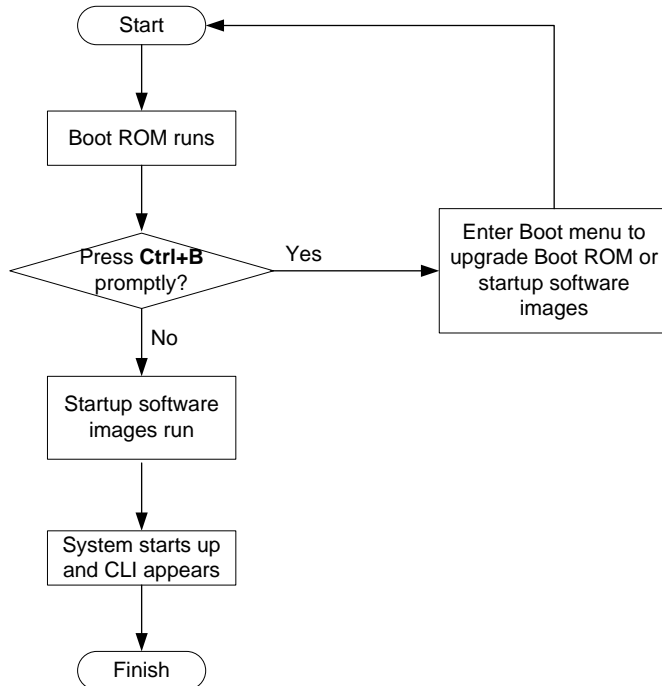
Boot ROM images are not released along with the boot images and system images. To get a version of Boot ROM image, contact the H3C technical support.

---

## 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, `5120v3-CMW710-BOOT-R6367.bin` and `5120v3-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
```

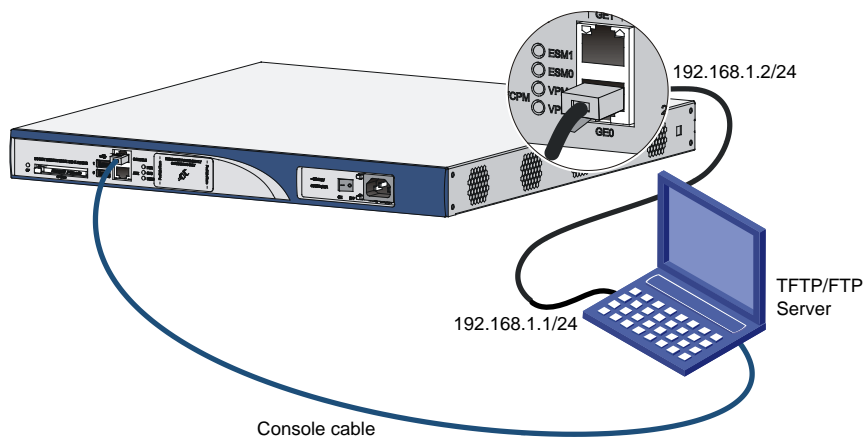
System state	:	Stable	
Redundancy state	:	No redundancy	
Slot	CPU	Role	State
1	0	Active	Stable
2. If the device is unstable, use the following commands to troubleshoot the issue:
  - Use the **display device** command to verify that the device is operating correctly.
  - Use the **display ha service-group** 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 5120v3 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 6](#).

**Table 6 Minimum free storage space requirements**

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

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 NW CW 5120v3 8G PoE+ 2 SFP 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 7 Shortcut keys**

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

# 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 8](#)). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE Networking Comware 5120v3 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 8 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 9</a> .
Ctrl+Y: Change Work Mode	Change Work Mode.
Ctrl+C: Display Copyright	Display the copyright statement.

**Table 9 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 10 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 11 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
```

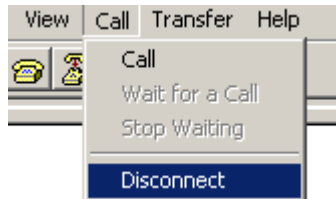
```
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
```



Press enter key when ready

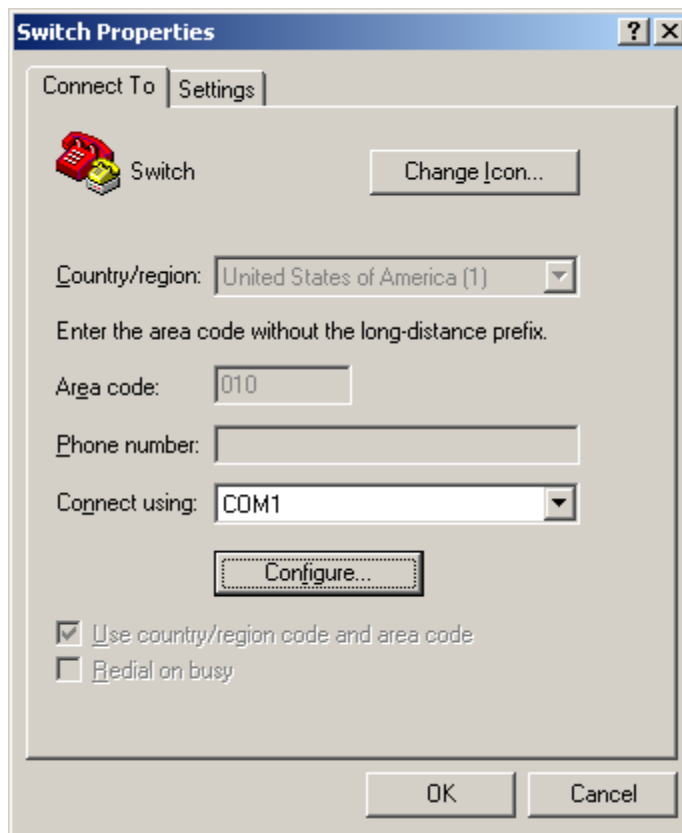
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
  - a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

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



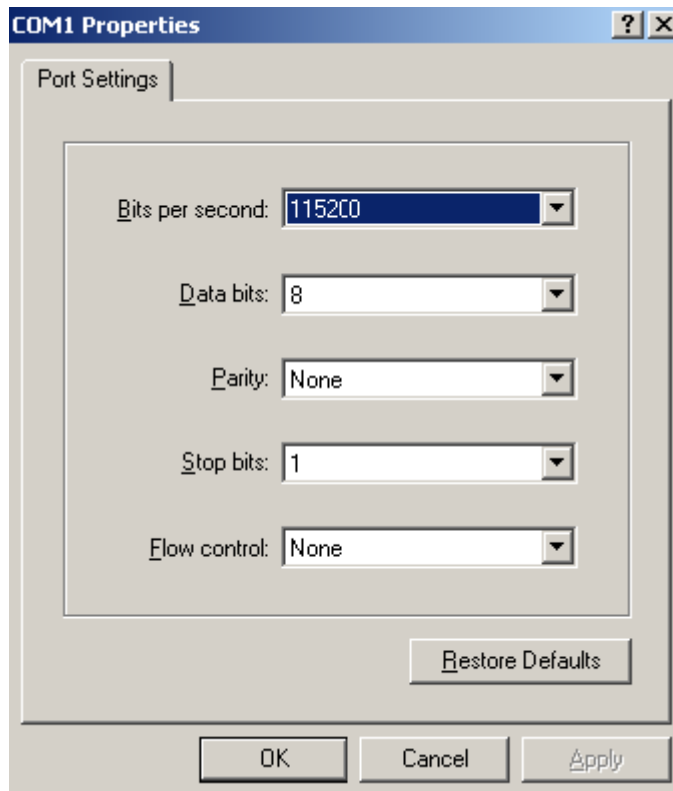
- b. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

**Figure 4 Properties dialog box**



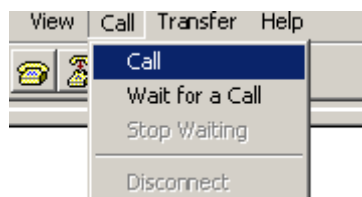
- c. Select **115200** from the **Bits per second** list and click **OK**.

**Figure 5 Modifying the baud rate**



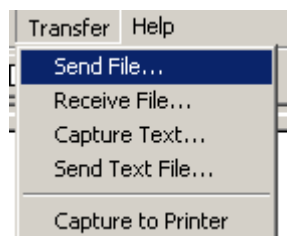
- d. Select **Call** > **Call** to reestablish the connection.

**Figure 6 Reestablishing the connection**



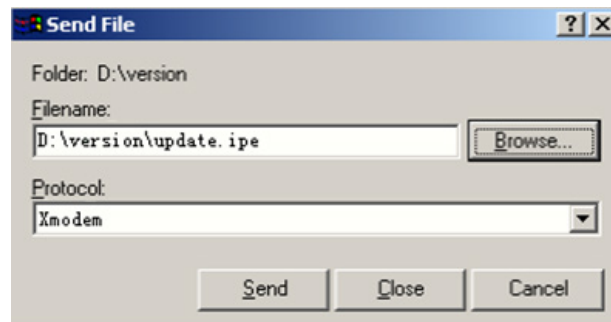
5. Press **Enter**. The following prompt appears:  
Are you sure to download file to flash? Yes or No (Y/N):Y
6. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)  
Now please start transfer file with XMODEM protocol  
If you want to exit, Press <Ctrl+X>  
Loading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

**Figure 7 Transfer menu**



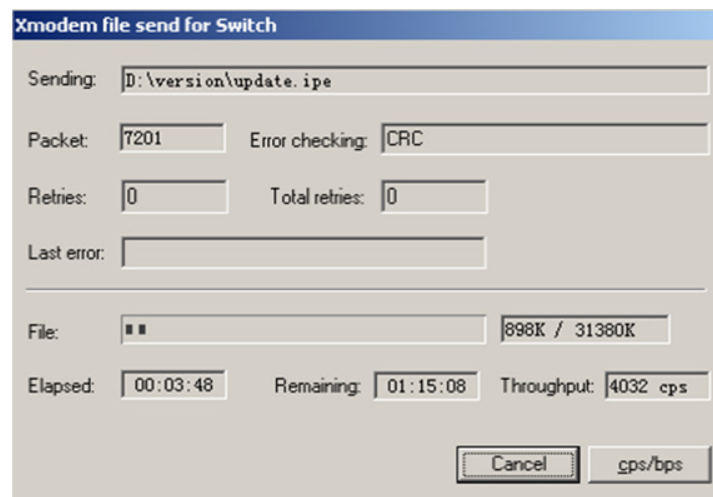
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

**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 12 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 13 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

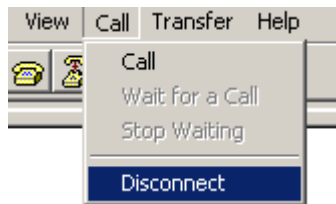
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

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.

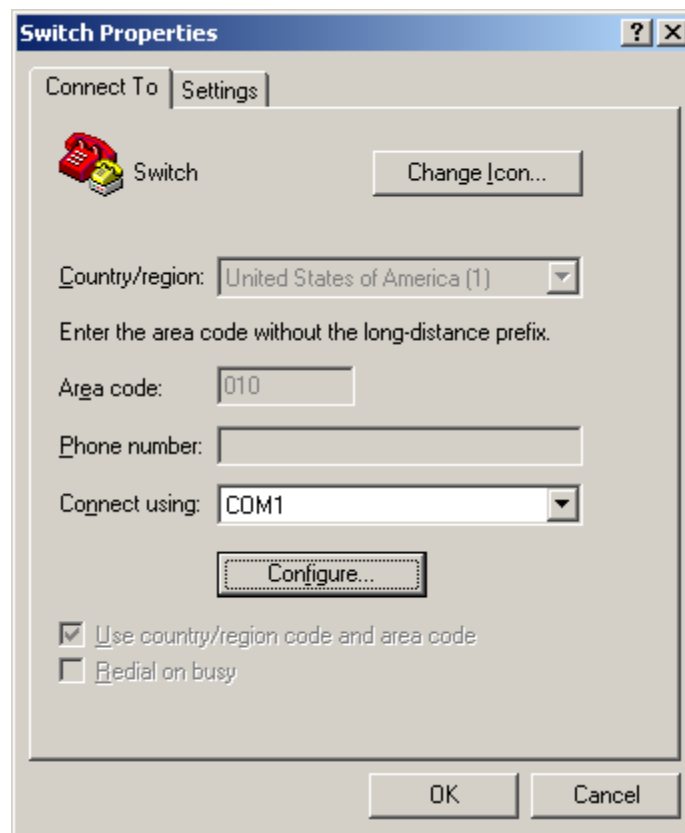
- a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

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



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

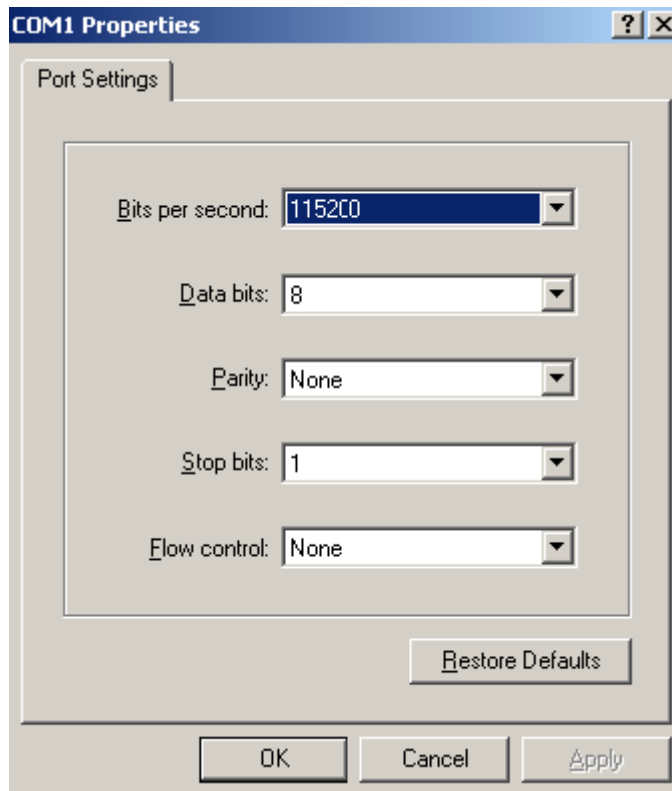
**Figure 11 Properties dialog box**



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

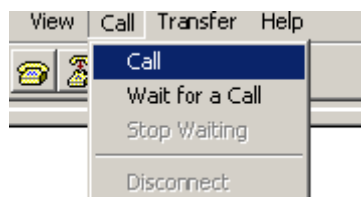


**Figure 12 Modifying the baud rate**



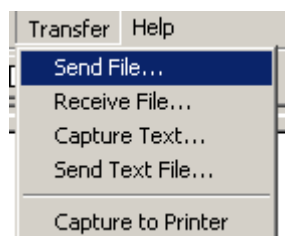
- d. Select **Call > Call** to reestablish the connection.

**Figure 13 Reestablishing the connection**



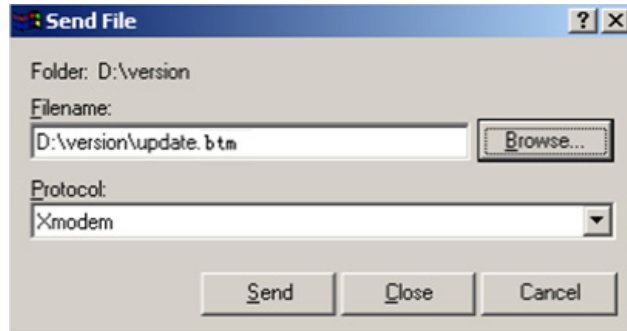
6. Press **Enter** to start downloading the file.  
Now please start transfer file with XMODEM protocol  
If you want to exit, Press <Ctrl+X>  
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
7. Select **Transfer > Send File** in the HyperTerminal window.

**Figure 14 Transfer menu**



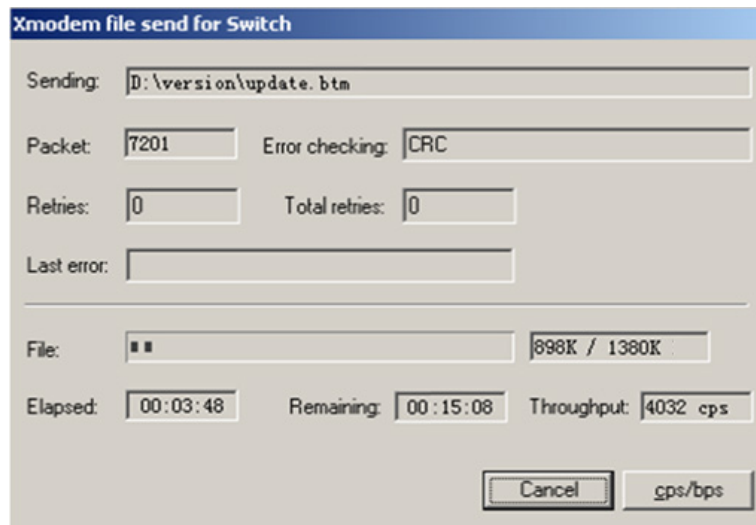
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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.



**Hewlett Packard**  
Enterprise

# HPE 5120v3-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  |
| New feature: Enabling port selection preemption on an aggregate interface ·                                         | 4  |
| Enabling port selection preemption on an aggregate interface.....                                                   | 4  |
| Command reference .....                                                                                             | 5  |
| lacp preempt delay.....                                                                                             | 5  |
| lacp preempt enable.....                                                                                            | 6  |
| New feature: Configuring an interface as an uplink interface to disable it from learning ARP snooping entries ..... | 6  |
| Configuring an interface as an uplink interface to disable it from learning ARP snooping entries .....              | 6  |
| Command reference .....                                                                                             | 7  |
| arp snooping uplink.....                                                                                            | 7  |
| New feature: Configuring spanning tree blackhole detection .....                                                    | 8  |
| Configuring spanning tree blackhole detection .....                                                                 | 8  |
| Command changes .....                                                                                               | 10 |
| display stp blackhole-detection blocked-port .....                                                                  | 10 |
| stp blackhole-detection enable.....                                                                                 | 11 |
| stp global blackhole-detection enable .....                                                                         | 13 |
| stp global blackhole-detection rx-bpdu timeout.....                                                                 | 14 |
| stp global timer blackhole-detection-interval .....                                                                 | 15 |
| stp global timer rx-blackhole-timeout .....                                                                         | 16 |
| stp timer blackhole-detection-interval.....                                                                         | 17 |
| stp timer rx-blackhole-timeout .....                                                                                | 18 |
| New feature: LLDP back hole detection .....                                                                         | 20 |
| Configuring LLDP black hole detection .....                                                                         | 20 |
| Command reference .....                                                                                             | 22 |
| lldp blackhole-detection enable.....                                                                                | 22 |
| lldp global blackhole-detection enable .....                                                                        | 24 |
| lldp global blackhole-detection rx-lldpdu timeout .....                                                             | 26 |
| lldp global timer blackhole-detection-interval .....                                                                | 27 |
| lldp global timer rx-blackhole-timeout.....                                                                         | 28 |
| lldp timer blackhole-detection-interval.....                                                                        | 29 |
| lldp timer rx-blackhole-timeout .....                                                                               | 30 |
| New feature: LLDP cross-domain detection .....                                                                      | 32 |
| Configuring LLDP cross-domain detection.....                                                                        | 32 |
| Command reference .....                                                                                             | 34 |
| lldp cross-domain-detection .....                                                                                   | 34 |
| lldp cross-domain-detection domain-id .....                                                                         | 35 |
| lldp global cross-domain-detection enable.....                                                                      | 37 |
| New feature: Using the subscriber ID as the client ID in all received DHCP requests.....                            | 39 |
| Using the subscriber ID as the client ID in all received DHCP requests .....                                        | 39 |
| Command reference .....                                                                                             | 40 |
| dhcp server subscriber-id replace client-id.....                                                                    | 40 |



|                                                                                                                              |           |
|------------------------------------------------------------------------------------------------------------------------------|-----------|
| dhcp server subscriber-id replace client-id global .....                                                                     | 41        |
| dhcp server subscriber-id interface-name .....                                                                               | 42        |
| <b>New feature: Configuring resource monitoring .....</b>                                                                    | <b>43</b> |
| Configuring resource monitoring .....                                                                                        | 43        |
| Command reference .....                                                                                                      | 44        |
| display resource-monitor .....                                                                                               | 44        |
| resource-monitor minor resend enable .....                                                                                   | 45        |
| resource-monitor output .....                                                                                                | 46        |
| resource-monitor resource .....                                                                                              | 46        |
| <b>New feature: Sending EAP-Success packets upon successful authorization in 802.1X .....</b>                                | <b>48</b> |
| Sending EAP-Success packets upon successful authorization .....                                                              | 48        |
| Command reference .....                                                                                                      | 49        |
| dot1x eap-success post-authorization .....                                                                                   | 49        |
| <b>Modified feature: Configuring the padding mode and padding format for the Circuit ID sub-option .....</b>                 | <b>50</b> |
| Feature change description .....                                                                                             | 50        |
| Command changes .....                                                                                                        | 50        |
| Modified command: dhcp relay information circuit-id .....                                                                    | 50        |
| <b>Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option .....</b>                  | <b>50</b> |
| Feature change description .....                                                                                             | 50        |
| Command changes .....                                                                                                        | 51        |
| Modified command: dhcp relay information remote-id .....                                                                     | 51        |
| <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 .....                                                                     | 52        |
| <b>Modified feature: Support for specifying a custom ASCII string as the client ID of a static binding .....</b>             | <b>53</b> |
| Feature change description .....                                                                                             | 53        |
| Modified command: static-bind .....                                                                                          | 53        |
| <b>Release 6352P02 .....</b>                                                                                                 | <b>54</b> |

# R6367

This release has the following changes:

- New Feature: Enabling port security unified secure MAC address control for access users
- 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: 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
- 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 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. <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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## 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.
  - o Enter Layer 2 aggregate interface view.  
**interface bridge-aggregation** *interface-number*
  - o 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
```

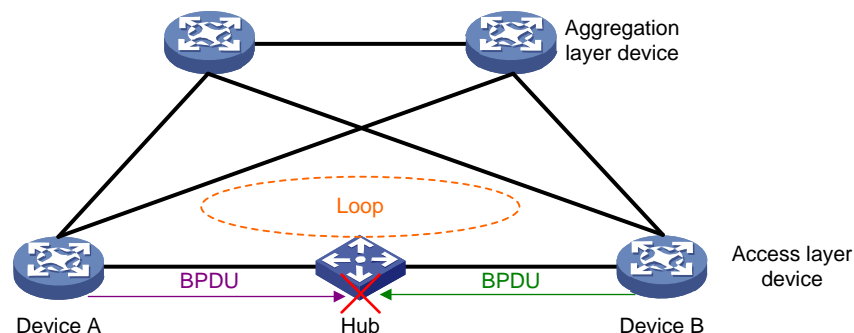
## New feature: Configuring spanning tree blackhole detection

### 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  
              Ten-GigabitEthernet3/0/1
```

**Table 2 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

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 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

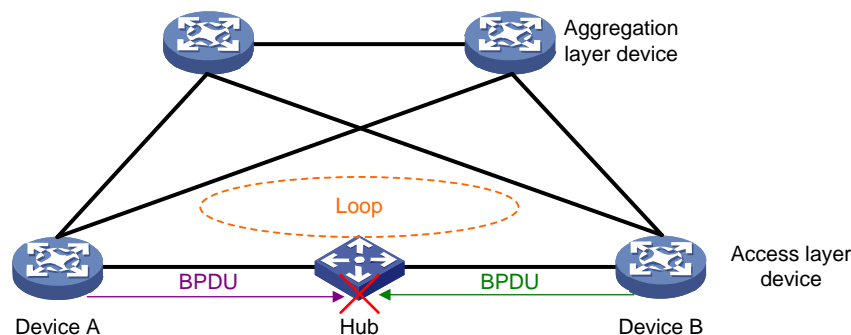
### Predefined user roles

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 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 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
```

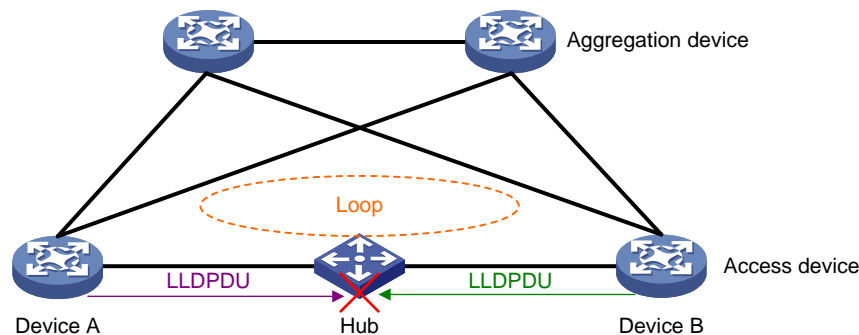
# New feature: LLDP black hole detection

## 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 is 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

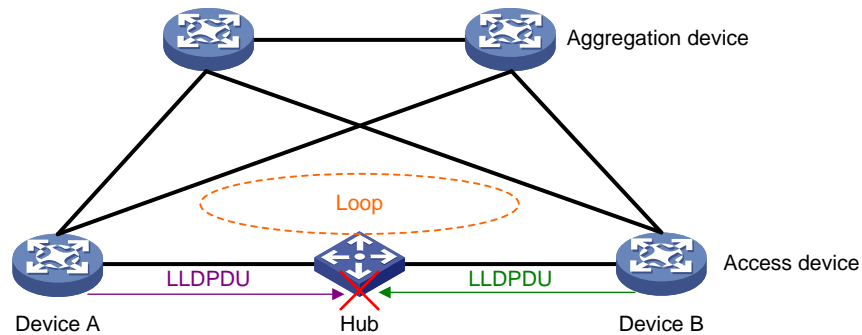
### Predefined user roles

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 is 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
```



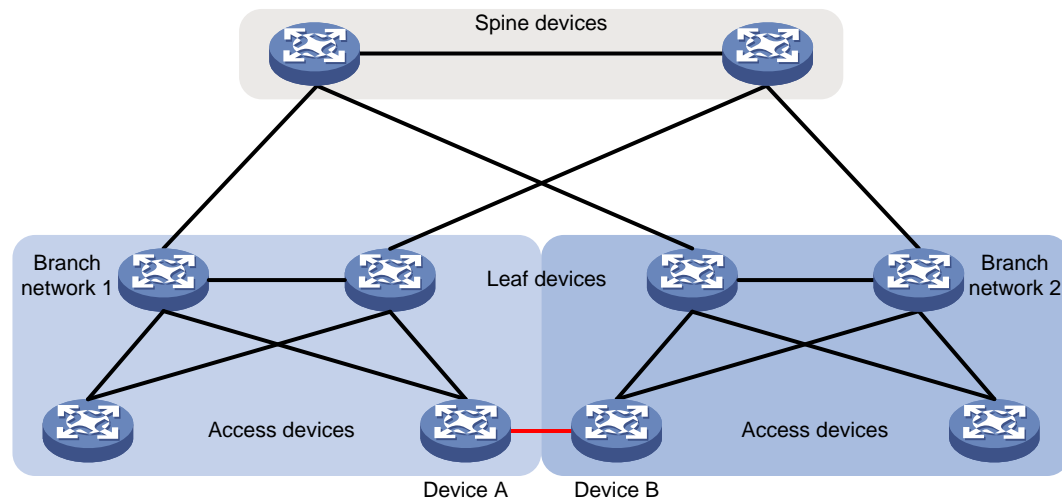
# New feature: LLDP cross-domain detection

## 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 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.

### 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

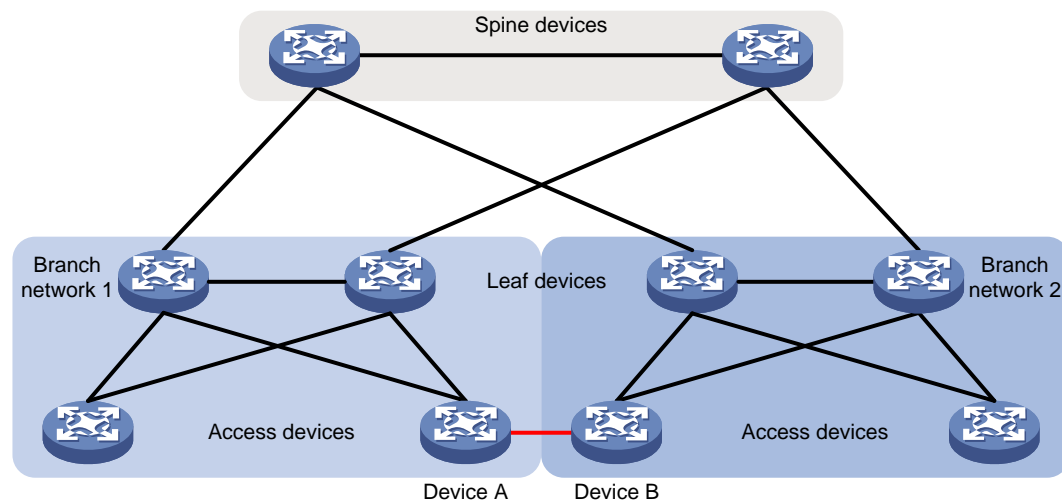
*domain-id*: Specifies a domain ID in the range of 1 to 10.

## 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.

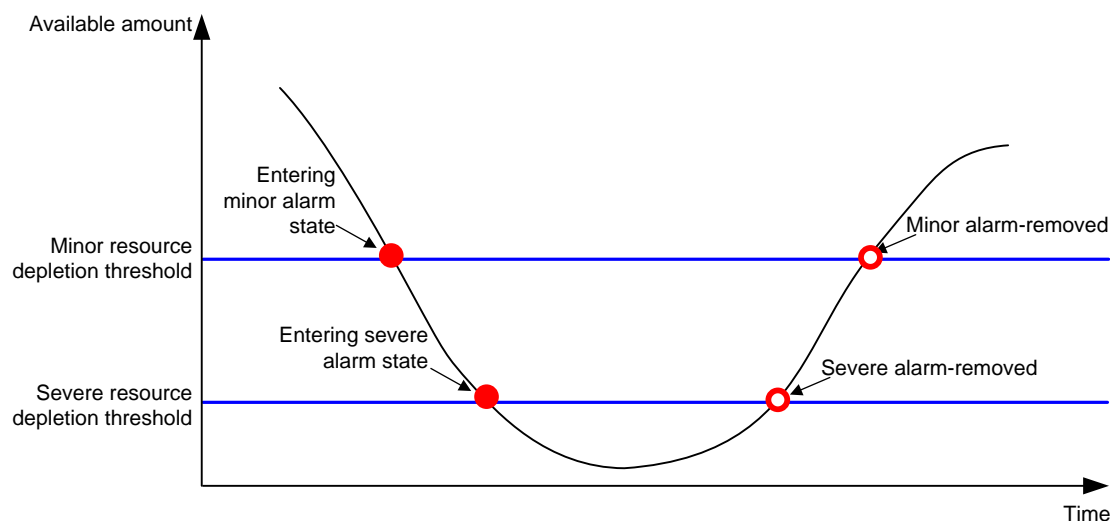
- If the available amount is equal to or less than the minor resource depletion threshold but greater than the severe resource depletion threshold, the resource type is in minor alarm state.
- If the available amount is equal to or less than the severe resource depletion threshold, the resource type 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 3 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 4 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: 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.

## 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 6352P02

This release has no feature changes.