



Hewlett Packard
Enterprise

HPE 5140EI-CMW710-R6343P09 Release Notes

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
5140EI-CMW710-R6343P09.....	3
5140EI-CMW710-R6343	3
5140EI-CMW710-R6337P01	3
5140EI-CMW710-R6330	3
5140EI-CMW710-R6327	3
5140EI-CMW710-R6325	3
Software feature and command updates	4
MIB updates.....	4
Operation changes	4
Operation changes in R6343P09	4
Operation changes in R6343.....	4
Operation changes in R6337P01	5
Operation changes in R6330.....	5
Operation changes in R6327.....	5
Operation changes in R6325.....	5
Restrictions and cautions	5
Restrictions.....	6
Cautions.....	6
Open problems and workarounds	6
List of resolved problems	6
Resolved problems in R6343P09.....	6
Resolved problems in R6343.....	6
Resolved problems in R6337P01	8
Resolved problems in R6330.....	10
Resolved problems in R6327.....	10
Resolved problems in R6325.....	11
Support and other resources.....	11
Accessing Hewlett Packard Enterprise Support.....	11

Documents	12
Related documents.....	12
Documentation feedback	12
Appendix A Feature list	13
Hardware features.....	13
Software features.....	17
Appendix B Fixed security vulnerabilities.....	20
Fixed security vulnerabilities in R6343.....	20
Appendix C Upgrading software	21
System software file types	21
System startup process.....	21
Upgrade methods	22
Preparing for the upgrade.....	23
Verifying device status	23
Setting up the upgrade environment	23
Upgrading from the CLI	24
Preparing for the upgrade	24
Downloading software images to the master switch	25
Upgrading from the Boot menu	29
Prerequisites	29
Accessing the Boot menu	30
Accessing the extended Boot menu	31
Upgrading Comware images from the Boot menu.....	32
Upgrading Boot ROM from the Boot menu	40
Managing files from the Boot menu.....	47
Handling software upgrade failures.....	50

List of tables

Table 1 Version history	1
Table 2 Hardware and software compatibility matrix	2
Table 3 MIB updates.....	4
Table 4 5140EI series hardware features for non-PoE switch models.....	13
Table 5 5140EI series hardware features for non-PoE switch models(2).....	14
Table 6 5140EI series hardware features for PoE switch models.....	15
Table 7 5140EI series hardware features for PoE switch models(2)	16
Table 8 Software features of the 5140EI series.....	17
Table 9 Minimum free storage space requirements.....	29
Table 10 Shortcut keys	30
Table 11 Extended Boot ROM menu options	31
Table 12 EXTENDED ASSISTANT menu options	32
Table 13 TFTP parameter description	33
Table 14 FTP parameter description.....	35
Table 15 TFTP parameter description	41
Table 16 FTP parameter description	42

Introduction

This document describes the features, restrictions and guidelines, open problems, and workarounds for version HPE 5140EI-CMW710-R6343P09. Before you use this version on a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HPE 5140EI-CMW710-R6343P09 Release Notes (Software Feature Changes)* and the documents listed in "[Related documents](#)."

Version information

Version number

HPE Comware Software, Version 7.1.070, Release 6343P09

Note: You can see the version number with the command **display version** in any view. Please see [Note ①](#).

Version history



IMPORTANT:

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

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
5140EI-CMW710-R6343P09	5140EI-CMW710-R6343	2022-11-30	Release version	Fixed bugs
5140EI-CMW710-R6343	5140EI-CMW710-R6337P01	2022-06-13	Release version	Fixed bugs
5140EI-CMW710-R6337P01	5140EI-CMW710-R6330	2021-12-09	Release version	Fixed bugs
5140EI-CMW710-R6330	5140EI-CMW710-R6327	2021-05-31	Release version	New feature
5140EI-CMW710-R6327	5140EI-CMW710-R6325	2021-03-01	Release version	Fixed bugs
5140EI-CMW710-R6325	First release	2020-12-25	Release version	First release

Hardware and software compatibility matrix



CAUTION:

To avoid an upgrade failure, use [Table 2](#) to verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix

Item	Specifications
Product family	5140EI Series
Hardware platform	HPE 5140 24G 4SFP+ EI Sw JL828A HPE 5140 24G SFP 4SFP+ EI Sw JL826A HPE 5140 48G 4SFP+ EI Sw JL829A HPE 5140 24G PoE+ 4SFP+ EI Sw JL827A HPE 5140 48G PoE+ 4SFP+ EI Sw JL824A HPE 5140 24G PoE+ 2SFP+ 2XGT EI Sw JL823A HPE 5140 48G PoE+ 2SFP+ 2XGT EI Sw JL825A HPE 5140 24G 2SFP+ 2XGT EI Sw R8J41A HPE 5140 8G 2SFP 2GT EI Sw R8J42A
Memory	512M
Flash	256M
Boot ROM version	Version 148 or higher (Note: Use the display version command in any view to view the version information. Please see Note②)
Software images and their MD5 checksums	5140EI-CMW710-R6343P09.ipe(See the MD5 file)
iMC版本号	iMC BIMS 7.3(E0506H01) iMC NTA 7.3 (E0707L06) iMC QoSM 7.3 (E0505P01) iMC SHM 7.3 (E0707L06) iMC PLAT 7.3(E0705P12) iMC EIA 7.3(E0611P13) iMC EAD 7.3(E0611P10)
iNode 版本号	iNode PC 7.3 (E0585)
Remarks	N/A

Display the system software and Boot ROM versions of 5140EI

```
<HPE>display version
```

```
HPE Comware Software, Version 7.1.070, Release 6343P09      -----Note①
Copyright (c) 2010-2022 Hewlett Packard Enterprise Development LP
HPE 5140 24G PoE+ 4SFP+ EI Sw uptime is 0 weeks, 0 days, 0 hours, 2 minutes
Last reboot reason : Cold reboot
```

```
Boot image: flash:/5140ei-cmw710-boot-r6343p09.bin
Boot image version: 7.1.070, Release 6343P09
Compiled Nov 08 2022 11:00:00
System image: flash:/5140ei-cmw710-system-r6343p09.bin
System image version: 7.1.070, Release 6343P09
Compiled Nov 08 2022 11:00:00
```

```
Slot 1:
```

```
Uptime is 0 weeks,0 days,0 hours,2 minutes
```

```

5140 24G PoE+ 4SFP+ EI Sw with 1 Processor
BOARD TYPE:          5140 24G PoE+ 4SFP+ EI Sw
DRAM:                512M bytes
FLASH:               256M bytes
PCB 1 Version:       VER.A
Bootrom Version:     148          -----Note②
CPLD 1 Version:      001
Release Version:     HPE 5140 24G PoE+ 4SFP+ EI Sw JL827A-6343P09
Patch Version  :     None
Reboot Cause   :     ColdReboot
[SubSlot 0] 20GE+4COMBO+4SFP Plus

```

Upgrade restrictions and guidelines

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

Hardware feature updates

5140EI-CMW710-R6343P09

None.

5140EI-CMW710-R6343

None.

5140EI-CMW710-R6337P01

None.

5140EI-CMW710-R6330

Support :

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

5140EI-CMW710-R6327

None.

5140EI-CMW710-R6325

First release.

Software feature and command updates

For more information about the software feature and command update history, see *HPE 5140_EI-CMW710-R6343P09 Release Notes (Software Feature Changes)*.

MIB updates

Table 3 MIB updates

Item	MIB file	Module	Description
5140EI-CMW710-R6343P09			
New	None	None	None
Modified	None	None	None
5140EI-CMW710-R6343			
New	None	None	None
Modified	None	None	None
5140EI-CMW710-R6337P01			
New	None	None	None
Modified	None	None	None
5140EI-CMW710-R6330			
New	None	None	None
Modified	None	None	None
5140EI-CMW710-R6327			
New	None	None	None
Modified	None	None	None
5140EI-CMW710-R6325			
New	First release	First release	First release
Modified	First release	First release	First release

Operation changes

Operation changes in R6343P09

None.

Operation changes in R6343

- The number of available ACL resources was increased from 512 to 768.
- Change for the **ipv6 verify source ip-address mac-address** command.

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

After modification: The device will generate **four** permit ACL rules for all configured interfaces globally and generate one deny ACL rule for each interface. The total number of used resources is the number of interfaces multiplied by 1 plus 4.

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

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

After modification: The device will generate **one** permit ACL rule for all configured interfaces globally and generate one deny ACL rule for each interface. The total number of used resources is the number of interfaces multiplied by 1 plus 1.

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

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

After modification: The device will generate **three** permit ACL rules for all configured interfaces globally and generate one deny ACL rule for each interface. The total number of used resources is the number of interfaces multiplied by 1 plus 3.

Operation changes in R6337P01

None.

Operation changes in R6330

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

Before modification: The packet loss duration is longer than 2000 milliseconds.

After modification: The packet loss duration is in the range of 200 to 500 milliseconds.

Operation changes in R6327

None.

Operation changes in R6325

First release.

Restrictions and cautions

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

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

Restrictions

Release 6343P09 must use BootROM 148 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.

This release does not support the operation changes in Release 6343.

Cautions

None.

Open problems and workarounds

None.

List of resolved problems

Resolved problems in R6343P09

202206140089

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

202208230885

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

202206210164

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

Resolved problems in R6343

202204210856

- Symptom: The fiber port of the combo port is up.

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

202205090269

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

202205050956

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

202204130283

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

202204080241

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

202203300985

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

202203170120

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

202201140229

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

202202231179

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

202203010889

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

202201250424

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

202201040567

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

202103250327

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

202112230657

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

Resolved problems in R6337P01

202111150249

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

202111050868

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

202109241082

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

202110090340

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

202110090688

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

202107050836

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

202109011682

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

202107211516

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

202106250033

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

202107290628

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

202104210763

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

202105310255

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

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

202104200312

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

Resolved problems in R6330

202104131824

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

202104190149

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

202105280911

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

202101181488

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

202101181303

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

Resolved problems in R6327

202101151443

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

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

202101130494

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

202101080488

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

202012241455

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

Resolved problems in R6325

First release.

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

Information to collect:

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

Documents

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

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

Related documents

The following documents provide related information:

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

Documentation feedback

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

Appendix A Feature list

Hardware features

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

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

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

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

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

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

Table 6 5140EI series hardware features for PoE switch models

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

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

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

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

	<ul style="list-style-type: none"> Max voltage: 90 VAC to 264 VAC @ 47 to 63 Hz 	
Maximum PoE power per port	30 W	
Total PoE power	370W	
Minimum power consumption	20W	32W
Maximum power consumption (including PoE power consumption)	450W	470W
Chassis leakage current compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	
Melting current of power module fuse	2 A/250 V	2 A/250 V
Cooling system	Using fixed fan trays to draw ambient air in from the left side and exhaust heated air from the right side	
Operating temperature	-5° C ~ 45° C (23°F to 113°F)	
Operating humidity	5% to 95%, noncondensing	
Fire resistance compliance	UL60950-1/EN60950-1/IEC60950-1/GB4943	

Software features

Table 8 Software features of the 5140EI series

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

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

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

Appendix B Fixed security vulnerabilities

Fixed security vulnerabilities in R6343

CVE-2022-0778

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

Appendix C Upgrading software

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

System software file types

Software required for starting up the switch includes:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the switch cannot correctly start up.
- **Software images**—Includes boot images and system images.
 - **Boot image**—A .bin file that contains the operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
 - **System image**—A .bin file that contains the minimum modules required for device operation and some basic features, including device management, interface management, configuration management, and routing management.

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

These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images in the file and sets them as startup software images. Typically, the Boot ROM and software images for this switch series are released in an .ipe file named **main.ipe**.

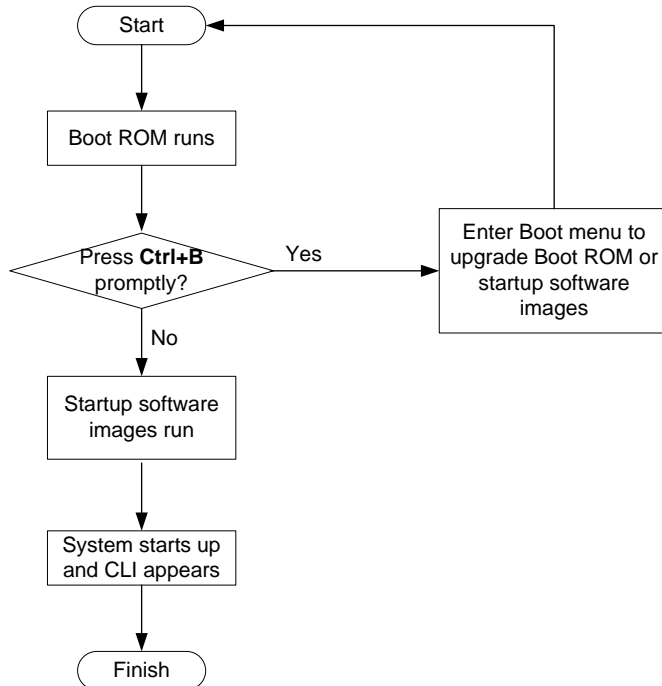
NOTE:

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

System startup process

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

Figure 1 System startup process



Upgrade methods

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

Upgrading method	Software types	Remarks
Upgrading from the CLI	<ul style="list-style-type: none">• Boot ROM image• Software images	<ul style="list-style-type: none">• You must reboot the switch to complete the upgrade.• This method can interrupt ongoing network services.
Upgrading from the Boot menu	<ul style="list-style-type: none">• Boot ROM image• Software images	<p>Use this method when the switch cannot correctly start up.</p> <p>⚠ CAUTION:</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, `5140_EI-CMW710-BOOT-R6343P09.bin` and `5140_EI-CMW710-SYSM-R6343P09.bin`.

Preparing for the upgrade

Verifying device status

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

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

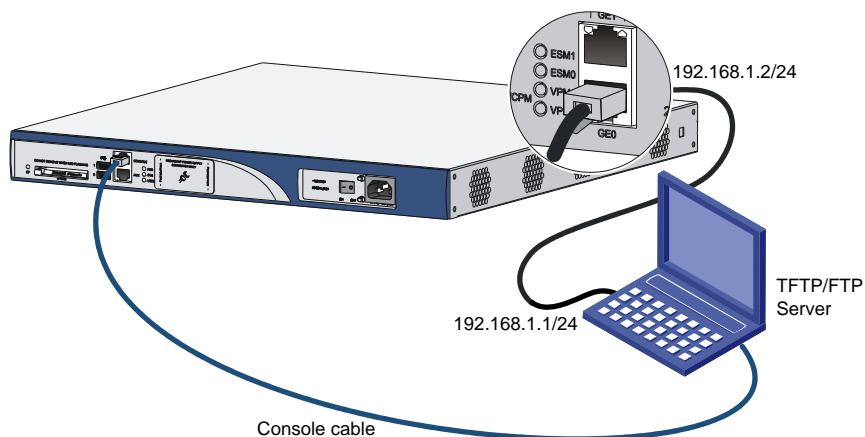
System state	:	Stable	
Redundancy state	:	No redundancy	
Slot	CPU	Role	State
1	0	Active	Stable
2. If the device is unstable, use the following commands to troubleshoot the issue:
 - Use the **display device** command to verify that the device is operating correctly.
 - Use the **display ha service-group**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

Setting up the upgrade environment

Before you upgrade system software, complete the following tasks:

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

Figure 2 Setting up the upgrade environment



Upgrading from the CLI

This section uses a two-member IRF fabric as an example to describe how to upgrade software from the CLI. If you have more than two subordinate switches, repeat the steps for the subordinate switch to upgrade their software. If you are upgrading a standalone switch, ignore the steps for upgrading the subordinate switch. For more information about setting up and configuring an IRF fabric, see the installation guide and IRF configuration guide for the HPE 5140EI switch series.

Preparing for the upgrade

Before you upgrade software, complete the following tasks:

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

```
<Sysname> display irf
```

MemberID	Role	Priority	CPU-Mac	Description
*+1	Master	5	0023-8927-afdc	---
2	Standby	1	0023-8927-af43	---

* indicates the device is the master.
+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 0023-8927-afdb

Auto upgrade : no
Mac persistent : 6 min
Domain ID : 0

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

❗ IMPORTANT:

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

Identify the free flash space of the master switch.

```
<Sysname> dir
```

Directory of flash:

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

251904 KB total (192736 KB free)

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

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

Directory of slot2#flash:/

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

```

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

```

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

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

CAUTION:

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

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

```

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

```

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

```

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

```

Downloading software images to the master switch

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

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

- [FTP download from a server](#)
- [FTP upload from a client](#)
- [TFTP download from a server](#)

Prerequisites

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

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

FTP download from a server

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

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

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

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

3. Enable the binary transfer mode.

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

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

```
ftp> get newest.ipe
227 Entering Passive Mode (10,10,110,1,17,97).
125 BINARY mode data connection already open, transfer starting for /newest.ipe
226 Transfer complete.
32133120 bytes received in 35 seconds (896.0 kbyte/s)
ftp> bye
221 Server closing.
```

FTP upload from a client

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

To FTP upload a file from a client:

On the IRF fabric:

1. Enable FTP server.

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

2. Configure a local FTP user account:

Create the user account.

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

Set its password and specify the FTP service.

```
[Sysname-luser-manage-abc] password simple pwd
```

```
[Sysname-luser-manage-abc] service-type ftp
```

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

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

```
[Sysname-luser-manage-abc] quit
```

```
[Sysname] quit
```

On the PC:

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

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1.
```

```

220 FTP service ready.
User(1.1.1.1:(none)):abc
331 Password required for abc.
Password:
230 User logged in.

```

4. Enable the binary file transfer mode.

```

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

```

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

```

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

```

TFTP download from a server

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

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

```
<Sysname> tftp 10.10.110.1 get newest.ipe
```

Press CTRL+C to abort.

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

Upgrading the software images

To upgrade the software images:

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

```
<Sysname> boot-loader file flash:/newest.ipe slot 1 main
```

Verifying the file flash:/newest.ipe on slot 1.....Done.

Images in IPE:

```
boot.bin
```

```
system.bin
```

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

Add images to slot 1.

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

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

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

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

The images that have passed all examinations will be used as the main startup software images at the next reboot on slot 1.

2. Specify the upgrade image file as the main startup image file for each subordinate switch. This example uses IRF member 2. (The subordinate switches will automatically copy the file to the root directory of their flash memories.)

```
<Sysname> boot-loader file flash:/newest.ipe slot 2 main
```

Verifying the file flash:/newest.ipe on slot 2.....Done.

Images in IPE:

```
boot.bin
system.bin
```

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

Add images to slot 2.

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

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

Verifying the file flash:/boot.bin on slot 2...Done.

Verifying the file flash:/system.bin on slot 2.....Done.

The images that have passed all examinations will be used as the main startup software images at the next reboot on slot 2.

3. Enable the software auto-update function.

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

```
[Sysname] irf auto-update enable
```

```
[Sysname] quit
```

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

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

```
<Sysname> save
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

flash:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait.....

Saved the current configuration to mainboard device successfully.

Slot 2:

Save next configuration file successfully.

5. Reboot the IRF fabric to complete the upgrade.

```
<Sysname> reboot
```

Start to check configuration with next startup configuration file, please wait.

.....DONE!

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

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

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

NOTE:

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

Upgrading from the Boot menu

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

**TIP:**

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

Prerequisites

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

Setting up the upgrade environment

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

NOTE:

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

3. Run a terminal emulator program on the console terminal and set the following terminal settings:
 - **Bits per second**—9,600
 - **Data bits**—8
 - **Parity**—None
 - **Stop bits**—1
 - **Flow control**—None
 - **Emulation**—VT100

Preparing for the TFTP or FTP transfer

To use TFTP or FTP:

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

Verifying that sufficient storage space is available

**IMPORTANT:**

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

When you upgrade software, make sure each member switch has sufficient free storage space for the upgrade file, as shown in [Table 9](#).

Table 9 Minimum free storage space requirements

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

Upgraded images	Minimum free storage space requirements
Boot ROM	Same size as the Boot ROM upgrade image file.

If no sufficient space is available, delete unused files as described in “[Managing files from the Boot menu.](#)”

Scheduling the upgrade time

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

Accessing the Boot menu

```
Starting.....
Press Ctrl+D to access BASIC BOOT MENU
Booting Normal Extend BootWare....

*****
*
*          HPE 5140 24G PoE+ 4SFP+ EI Sw BOOTROM, Version 148          *
*
*****

Copyright (c) 2010-2022 Hewlett Packard Enterprise Development LP

Creation Date       : Nov 30 2022, 11:46:20
CPU Clock Speed    : 800MHz
Memory Size        : 512MB
Flash Size         : 256MB
CPLD Version       : 001
PCB Version        : Ver.A
Mac Address        : aa1122334455
Press Ctrl+B to access EXTENDED BOOT MENU...1
```

Press one of the shortcut key combinations at prompt.

Table 10 Shortcut keys

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

Accessing the extended Boot menu

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

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

The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the extended Boot menu. Availability of some menu options depends on the state of password recovery capability (see [Table 11](#)). For more information about password recovery capability, see *Fundamentals Configuration Guide* in *HPE FlexNetwork 5140 EI Switch Series Configuration Guides-R63xx*.

Password recovery capability is enabled.

```
EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright

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

Table 11 Extended Boot ROM menu options

Option	Tasks
1. Download image to flash	Download a software image file to the flash.
2. Select image to boot	<ul style="list-style-type: none">Specify the main and backup software image file for the next startup.Specify the main and backup configuration files for the next startup. This task can be performed only if password recovery capability is enabled.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.

Option	Tasks
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.
Ctrl+F: Format file system	Format the current storage medium.
Ctrl+P: Change authentication for console login	Skip the authentication for console login. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
Ctrl+R: Download image to SDRAM and run	Download a system software image and start the switch with the image. This option is available only if password recovery capability is enabled.
Ctrl+Z: Access EXTENDED ASSISTANT MENU	Access the EXTENDED ASSISTANT MENU. For options in the menu, see Table 12 .
Ctrl+Y: Change Work Mode	Change Work Mode.
Ctrl+C: Display Copyright	Display the copyright statement.

Table 12 EXTENDED ASSISTANT menu options

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

Upgrading Comware images from the Boot menu

You can use the following methods to upgrade Comware images:

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

Using TFTP to upgrade software images through the Ethernet port

1. Enter **1** in the Boot menu to access the file transfer protocol submenu.
 1. Set TFTP protocol parameters
 2. Set FTP protocol parameters
 3. Set XMODEM protocol parameters
 0. Return to boot menu

Enter your choice(0-3):

2. Enter 1 to set the TFTP parameters.

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

Table 13 TFTP parameter description

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

NOTE:

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

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

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

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

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

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

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

NOTE:

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

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

EXTENDED BOOT MENU

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

Enter your choice(0-8): 0

Using FTP to upgrade software images through the Ethernet port**1. Enter 1 in the Boot menu to access the file transfer protocol submenu.**

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

Enter your choice(0-3):

2. Enter 2 to set the FTP parameters.

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

Table 14 FTP parameter description

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

NOTE:

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

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

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

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

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

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

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

EXTENDED BOOT MENU

```

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
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.

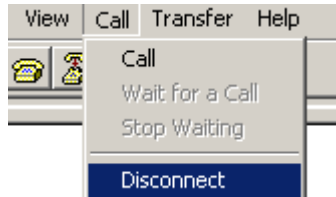
Download baudrate is 115200 bps

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

Press enter key when ready

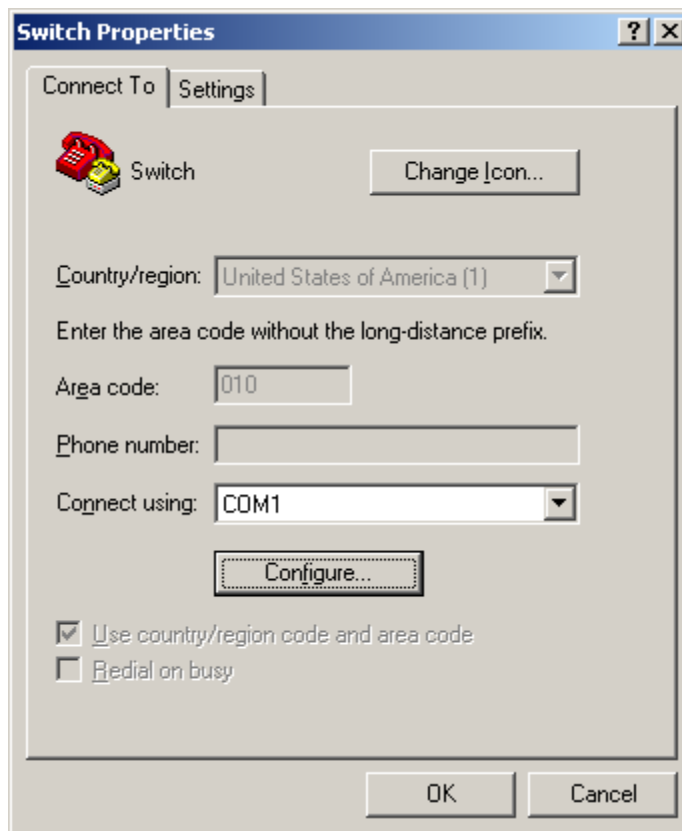
4. Set the serial port on the terminal to use the same baud rate and protocol as the console port. If you select 9600 bps as the download rate for the console port, skip this task.
 - a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 3 Disconnecting the terminal from the switch



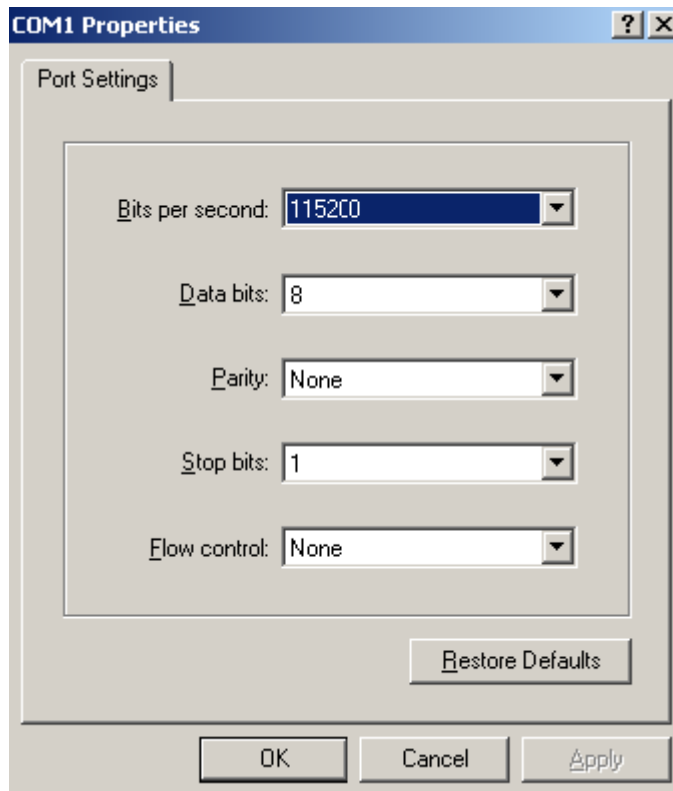
- b. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 4 Properties dialog box



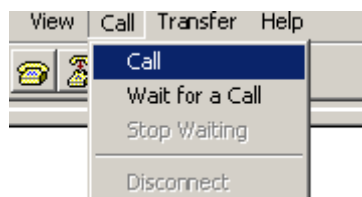
- c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 5 Modifying the baud rate



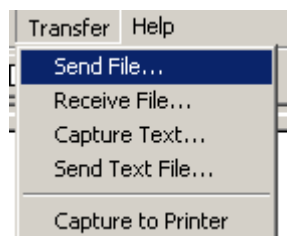
- d. Select **Call > Call** to reestablish the connection.

Figure 6 Reestablishing the connection



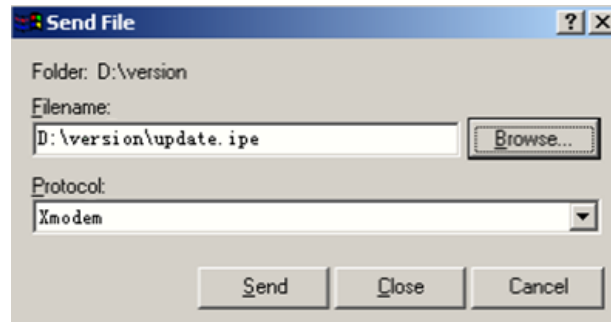
5. Press **Enter**. The following prompt appears:
`Are you sure to download file to flash? Yes or No (Y/N):Y`
6. Enter **Y** to start downloading the file. (To return to the Boot menu, enter **N**.)
`Now please start transfer file with XMODEM protocol`
`If you want to exit, Press <Ctrl+X>`
`Loading ...CCCCCCCCCCCCCCCCCCCCCCCCCCCC`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

Figure 7 Transfer menu



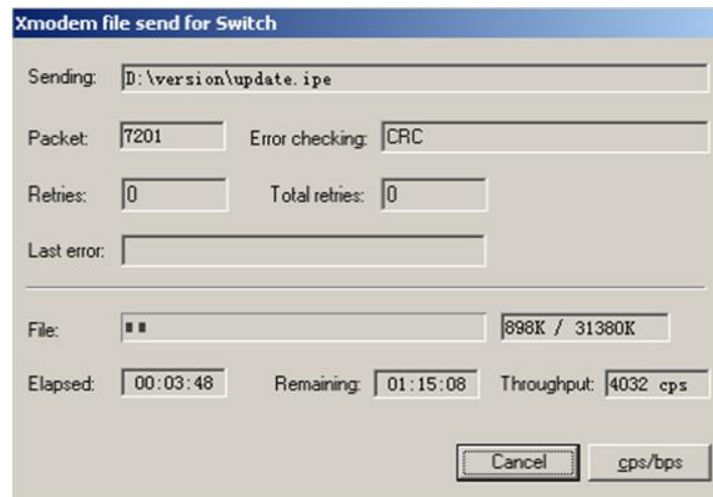
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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

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

NOTE:

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

EXTENDED BOOT MENU

```
1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot

Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+Y: Change Work Mode
Ctrl+C: Display Copyright
```

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

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

Upgrading Boot ROM from the Boot menu

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

- [Using TFTP to upgrade Boot ROM through the Ethernet port](#)
- [Using FTP to upgrade Boot ROM through the Ethernet port](#)
- [Using XMODEM to upgrade Boot ROM through the console port](#)

Using TFTP to upgrade Boot ROM through the Ethernet port

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

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

Enter your choice(0-3):

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

The file transfer protocol submenu appears:

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

Enter your choice(0-3):

3. Enter 1 to set the TFTP parameters.

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

Table 15 TFTP parameter description

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

NOTE:

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

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

Loading.....Done!

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

Will you Update Basic BootRom? (Y/N):Y

Updating Basic BootRom.....Done.

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

Updating extended BootRom? (Y/N):Y

Updating extended BootRom.....Done.

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

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

Enter your choice(0-3):

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

Using FTP to upgrade Boot ROM through the Ethernet port

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

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

Enter your choice(0-3):

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

The file transfer protocol submenu appears:

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

Enter your choice(0-3):

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

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

Table 16 FTP parameter description

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

NOTE:

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

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

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

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

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

Updating Basic BootRom.....Done.

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

Updating extended BootRom? (Y/N):Y

Updating extended BootRom.....Done.

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

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

Enter your choice(0-3):

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

Using XMODEM to upgrade Boot ROM through the console port

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

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

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

Enter your choice(0-3):

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

The file transfer protocol submenu appears:

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

Enter your choice(0-3):

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

Please select your download baudrate:

- 1.* 9600
2. 19200
3. 38400
4. 57600
5. 115200
0. Return to boot menu

Enter your choice(0-5):5

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

Download baudrate is 115200 bps

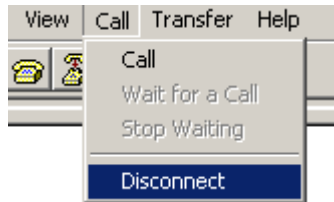
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol

Press enter key when ready

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

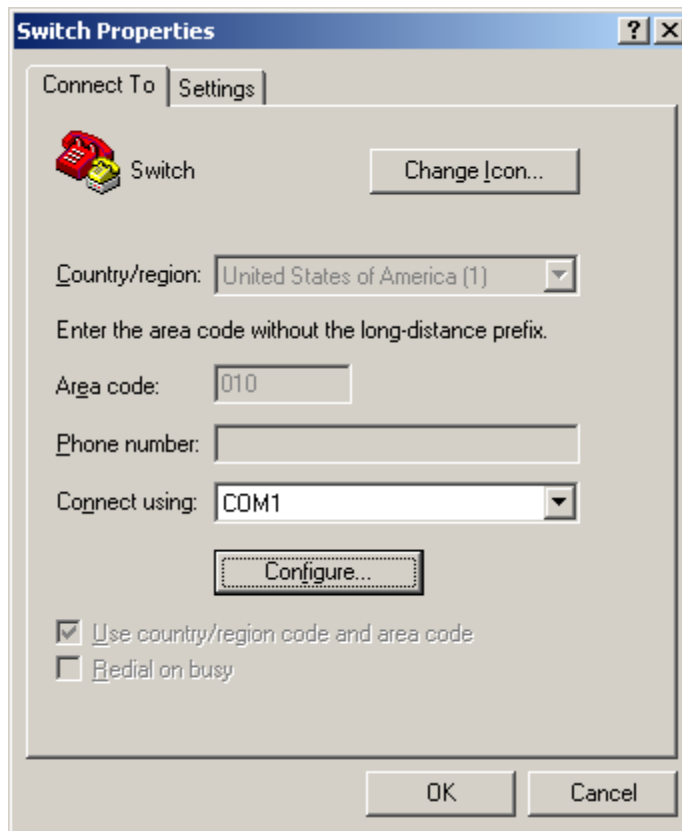
- a. Select **Call > Disconnect** in the HyperTerminal window to disconnect the terminal from the switch.

Figure 10 Disconnecting the terminal from the switch



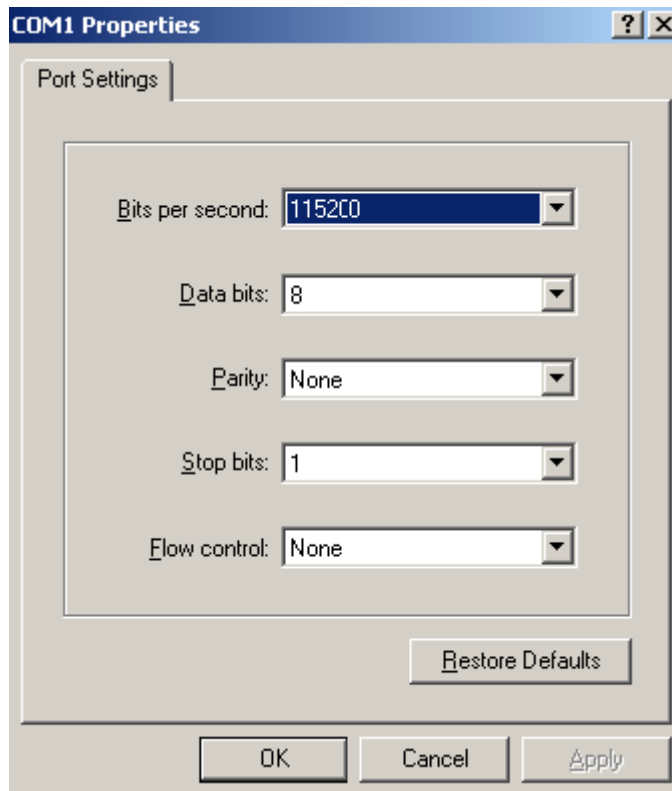
- b. Select **File > Properties**, and in the **Properties** dialog box, click **Configure**.

Figure 11 Properties dialog box



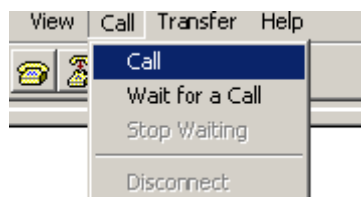
- c. Select **115200** from the **Bits per second** list and click **OK**.

Figure 12 Modifying the baud rate



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

Figure 13 Reestablishing the connection

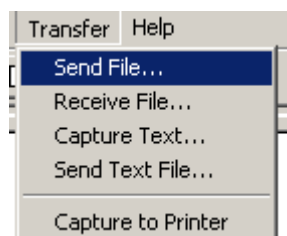


6. Press **Enter** to start downloading the file.

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

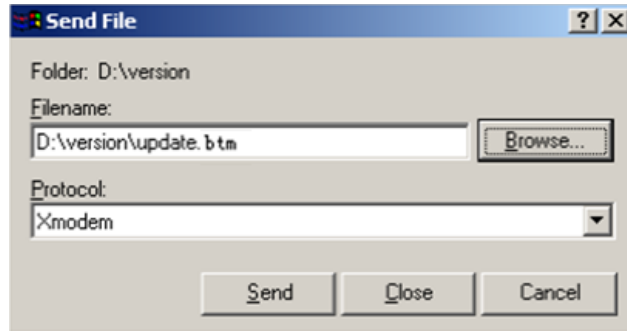
7. Select **Transfer > Send File** in the HyperTerminal window.

Figure 14 Transfer menu



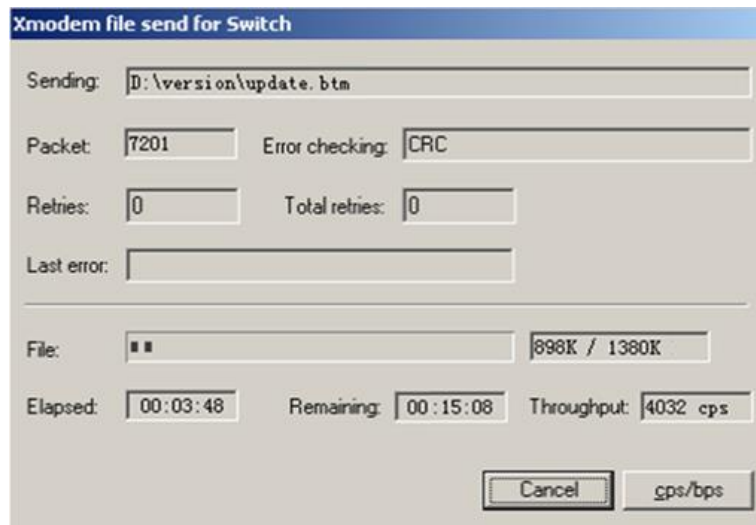
8. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

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 ...CCCCCCCCCCCCCCC ...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 5140_EI-CMW710-R6343P09 Release Notes

Software Feature Changes

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

© Copyright 2022 Hewlett Packard Enterprise Development LP

Contents

Release 6343P09	1
Modified feature: Factory defaults change for console login and password control settings	1
Feature change description.....	1
Command changes.....	2
Release 6343	1
New feature: Configuring interface alarm functions.....	1
Command changes	2
ifmonitor input-error.....	2
ifmonitor output-error.....	3
port ifmonitor input-error.....	4
port ifmonitor output-error	5
Modified command: snmp-agent trap enable ifmonitor.....	6
New feature: Configuring the aging timer for temporary MAC address entries for Web authentication	7
Command reference	8
New command: web-auth timer temp-entry-aging	8
Modified command: display web-auth.....	9
Modified feature: Displaying the running configuration.....	9
Feature change description.....	9
Command changes	9
Modified command: display current-configuration.....	9
Modified feature: Displaying the running configuration in current view	10
Feature change description.....	10
Command changes	10
Modified command: display this	10
Modified feature: 802.1X periodic reauthentication timer	10
Feature change description.....	10
Command changes	10
Modified command: dot1x timer reauth-period (system view).....	10
Modified command: dot1x timer reauth-period (interface view)	11
Modified feature: Periodic MAC reauthentication timer	11
Feature change description.....	11
Command changes	11
Modified command: mac-authentication timer (system view)	11
Modified command: mac-authentication timer (interface view).....	11
Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option of Option 82.....	12
Feature change description.....	12
Command changes	12
Modified command: dhcp relay information remote-id	12
Modified feature: Configuring gRPC collectors	12
Feature change description.....	12
Command changes	13
New command: domain-name	13

New command: ipv6 domain-name.....	14
Modified command: display grpc.....	15
Modified feature: Displaying detailed information about 802.1X online users	16
Feature change description.....	16
Command changes.....	16
Modified command: display dot1x connection	16
Release 6337P01	1
New feature: Configuring SmartMC	1
About SmartMC.....	1
SmartMC network framework.....	1
SmartMC network establishment	2
SmartMC features	3
Restrictions: Hardware compatibility with SmartMC	6
Restrictions and guidelines: SmartMC configuration	6
SmartMC tasks at a glance	6
Prerequisites for SmartMC.....	7
Enabling SmartMC	7
Setting the file server information	8
Configuring an outgoing interface for the SmartMC network	9
Enabling automatic Ethernet link aggregation	9
Modifying the password of the default user for members	9
Creating a SmartMC group	10
Creating a VLAN for members.....	10
Deploying a batch file to members.....	11
Configuring a batch file for ports connecting APs or IP phones.....	11
Backing up configuration files	11
Configuring resource monitoring.....	12
Upgrading the startup software and configuration file on members.....	13
About upgrading the startup software and configuration file on members	13
Restrictions and guidelines for startup software and configuration file upgrade	13
Prerequisites	13
Upgrading the startup software and configuration file on members.....	13
Upgrading the startup software and configuration file on all members in SmartMC groups	14
Managing the network topology	15
Refreshing the network topology.....	15
Saving the network topology.....	16
Replacing faulty members.....	16
Display and maintenance commands for SmartMC.....	17
SmartMC configuration examples	17
Example: Configuring SmartMC.....	17
Command reference	20
boot-loader file	20
create batch-file.....	21
display smartmc backup configuration status	22
display smartmc batch-file status	23
display smartmc configuration.....	24
display smartmc device-link	26
display smartmc group	26
display smartmc replace status.....	28
display smartmc resource-monitor	28
display smartmc resource-monitor configuration	29
display smartmc tc	30
display smartmc tc log buffer	32
display smartmc tc log restart	33
display smartmc upgrade status	34
display smartmc vlan.....	35
match	36
smartmc auto-link-aggregation enable.....	36
smartmc auto-replace enable.....	37

smartmc backup configuration	38
smartmc backup configuration max-number	38
smartmc backup configuration interval	39
smartmc batch-file apply	40
smartmc batch-file deploy	41
smartmc batch-file-apply enable	41
smartmc enable	42
smartmc { ftp-server sftp-server }	43
smartmc group	44
smartmc outbound	45
smartmc resource-monitor	45
smartmc resource-monitor interval	47
smartmc resource-monitor max-age	47
smartmc replace	48
smartmc tc boot-loader	49
smartmc tc device-type	49
smartmc tc password	50
smartmc tc startup-configuration	51
smartmc topology-refresh	51
smartmc topology-refresh interval	52
smartmc topology-save	52
smartmc upgrade boot-loader	53
smartmc upgrade startup-configuration	54
smartmc vlan	55
startup-configuration	56
New feature: Configuring interface alarm functions	58
Configuring interface alarm functions	58
Command reference	59
ifmonitor crc-error	59
port ifmonitor crc-error	60
snmp-agent trap enable ifmonitor	61
New feature: Configuring Option 60 for DHCP requests	61
Configuring Option 60 for DHCP requests	61
Command reference	62
dhcp client class-id	62
New feature: Configuring the type of port ID TLVs advertised by LLDP	63
Configuring the type of port ID TLVs advertised by LLDP	63
Command reference	64
lldp global tlv-config basic-tlv port-id	64
lldp tlv-config basic-tlv port-id	64
New feature: Enabling displaying LLDP local information about all interfaces	65
Enabling displaying LLDP local information about all interfaces	65
Command reference	66
lldp local-information all-interface	66
New feature: PoE forced power supply	67
Enabling PoE forced power supply	67
Command reference	67
poe force-power	67
Command changes	68
Modified command: display poe pse	68
New feature: Interval at which the SNMP module examines the system configuration for changes	69
Setting the interval at which the SNMP module examines the system configuration for changes	69
Command reference	69

snmp-agent configuration-examine interval	69
New feature: Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users	70
Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users.....	70
dot1x { ip-verify-source ipv6-verify-source } enable	71
New feature: Automated IPv6 underlay network deployment for VCF fabric	71
About automated IPv6 underlay network deployment	71
Command reference	72
Modified feature: Setting the port status detection timer	72
Feature change description.....	72
Command changes.....	72
Modified command: shutdown-interval.....	72
Modified feature: 802.1X EAD assistant.....	72
Feature change description.....	72
Command changes	72
New command: dot1x ead-assistant permit authentication-escape.....	72
Modified feature: Displaying information about online 802.1X users	73
Feature change description.....	73
Command changes	73
Modified command: display dot1x connection	73
Modified feature: Displaying information about online MAC authentication users.....	74
Feature change description.....	74
Command changes	74
Modified command: display mac-authentication connection.....	74
Modified feature: L2PT for CFD	75
Feature change description.....	75
Command changes	75
Modified command: l2protocol type tunnel-dmac.....	75
Modified command: l2protocol tunnel dot1q	76
Modified command: display l2protocol statistics	77
Release 6330	79
New feature: Enabling fast PoE for a PSE	79
Enabling fast PoE for a PSE	79
Command reference	79
poe fast-on enable	79
Modified feature: L2PT for CFD and DTP	80
Feature change description.....	80
Command changes	80
New command: l2protocol type tunnel-dmac	80
Modified command: l2protocol tunnel dot1q	81
Modified command: display l2protocol statistics	82
Modified feature: Displaying information about online 802.1X users	83
Feature change description.....	83
Command changes	83
Modified command: display dot1x connection	83

Modified feature: Displaying information about online MAC authentication
users..... 84

 Feature change description..... 84

 Command changes 84

 Modified command: display mac-authentication connection..... 84

Release 6343P09

This release has the following changes:

- Modified feature: Factory defaults change for console login and password control settings

Modified feature: Factory defaults change for console login and password control settings

Feature change description

Factory defaults are custom basic settings that came with the device. You can use the display default-configuration command to display factory defaults.

The device starts up with the factory defaults if no next-startup configuration files are available.

In this version, the following factory default settings are added:

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

The output shows that the factory defaults for console login and password control settings change:

- The device performs local AAA authentication for console users. A console user must use the username admin without any password to log in to the device for the first time. The user role network-admin is assigned to the login console user.
- By default, the global password control and password change at first login are both enabled. Users must change the password at first login before they can access the system. The new password must contain a minimum of four different characters.

- The default maximum account idle time is 0 days. The system has no restriction for the account idle time.
- The default minimum password update interval is 0 hours. The system has no requirement for the password update interval.
- The default maximum number of consecutive login failures is 3. When console user fails the maximum number of login attempts, the console user can continue using this user account to make login attempts.
- After a console user modifies the password after first login, if you want to delete the default user account admin, make sure either of the following conditions are met before deleting the user account admin:
 - Another user account with the highest permissions exists.
 - The authentication-mode none command has been configured for AUX user lines.
- If you add or modify security configurations, make sure they do not conflict with the factory defaults or will not lead login failures. For more information about factory defaults, see configuration file management in Fundamentals Configuration Guide for the product. For more information about AAA authentication and password control, see Security Configuration Guide.
- After the global password control is enabled, the device generates an lauth.dat file to save the authentication and login information for local users. Do not edit or delete this file to ensure the authentication and login of the local users.
 - If you execute the restore factory-default command in user view to restore the factory defaults, the lauth.dat file will be deleted. After the device reboots, you can use the username admin without any password to log in to the device, and you are required to change the password.
 - If you restore the factory defaults through Restore to factory default configuration on the boot menu, the lauth.dat file will not be deleted. After the device reboots, you must use the latest password to log in to the device.

Command changes

None.

Release 6343

This release has the following changes:

- New feature: Configuring interface alarm functions
- New feature: Configuring the aging timer for temporary MAC address entries for Web authentication
- Modified feature: Displaying the running configuration
- Modified feature: Displaying the running configuration in current view
- Modified feature: 802.1X periodic reauthentication timer
- Modified feature: Periodic MAC reauthentication timer
- Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option of Option 82
- Modified feature: Configuring gRPC collectors
- Modified feature: Displaying detailed information about 802.1X online users

New feature: Configuring interface alarm functions

About this task

With the interface alarm functions enabled, when the number of error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

Restrictions and guidelines

You can configure the error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

An interface that is shut down because of error packet alarms cannot automatically recover. To bring up the interface, execute the **undo shutdown** command on the interface.

Configuring input error packet alarm parameters

1. Enter system view.

```
system-view
```

2. Configure global input error packet alarm parameters.

```
ifmonitor input-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [ shutdown ]
```

By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packets.

3. Enter Ethernet interface view.

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

4. Configure input error packet alarm parameters for the interface.

```
port ifmonitor input-error high-threshold high-value low-threshold  
low-value interval interval [ shutdown ]
```

By default, an interface uses the global input error packet alarm parameters.

Configuring output error packet alarm parameters

1. Enter system view.

```
system-view
```

2. Configure global output error packet alarm parameters.

```
ifmonitor output-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown]
```

By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packets.

3. Enter Ethernet interface view.

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

4. Configure output error packet alarm parameters.

```
port ifmonitor output-error high-threshold high-value low-threshold  
low-value interval interval [shutdown]
```

By default, an interface uses the global output error packet alarm parameters.

Command changes

ifmonitor input-error

Use **ifmonitor input-error** to configure global input error packet alarm parameters.

Use **undo ifmonitor input-error** to restore the default.

Syntax

```
ifmonitor input-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown]
```

```
undo ifmonitor input-error slot slot-number
```

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for input error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this

keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms.

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

```
[Sysname] ifmonitor input-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

ifmonitor output-error

Use **ifmonitor output-error** to configure global output error packet alarm parameters.

Use **undo ifmonitor output-error** to restore the default.

Syntax

```
ifmonitor output-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown]
```

```
undo ifmonitor output-error slot slot-number
```

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for output error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms.

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

```
[Sysname] ifmonitor output-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

```
snmp-agent trap enable ifmonitor
```

port ifmonitor input-error

Use **port ifmonitor input-error** to configure input error packet alarm parameters for an interface.

Use **undo port ifmonitor input-error** to restore the default.

Syntax

```
port ifmonitor input-error high-threshold high-value low-threshold low-value interval interval [ shutdown ]
```

```
undo port ifmonitor input-error
```

Default

An interface uses the global input error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for input error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for input error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of input error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of input error packets exceeds the upper threshold on the interface.

Usage guidelines

With the input error packet alarm function enabled, when the number of input error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of input error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the input error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for input error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor input-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

port ifmonitor output-error

Use **port ifmonitor output-error** to configure output error packet alarm parameters for an interface.

Use **undo port ifmonitor output-error** to restore the default.

Syntax

port ifmonitor output-error high-threshold *high-value* **low-threshold** *low-value* **interval** *interval* [**shutdown**]

undo port ifmonitor output-error

Default

An interface uses the global output error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for output error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for output error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of output error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of output error packets exceeds the upper threshold on the interface.

Usage guidelines

With the output error packet alarm function enabled, when the number of output error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of output error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the output error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces. The configuration in interface view takes effect only on the current interface. (Devices that do not support the **slot** keyword.)
- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for output error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor output-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

Modified command: snmp-agent trap enable ifmonitor

Old syntax

```
snmp-agent trap enable ifmonitor [ crc-error ]
undo snmp-agent trap enable ifmonitor [ crc-error ]
```

New syntax

```
snmp-agent trap enable ifmonitor [ crc-error | input-error | output-error ]  
*  
undo snmp-agent trap enable ifmonitor [ crc-error | input-error |  
output-error ] *
```

Views

System view

Change description

Before modification: SNMP notifications for input and output error packets is not supported.

After modification: SNMP notifications for input and output error packets is supported.

New feature: Configuring the aging timer for temporary MAC address entries for Web authentication

About this task

If Web authentication is enabled, the device generates a temporary MAC address entry when it detects traffic from a user for the first time. The entry records the MAC address, access interface, and VLAN ID of the user, as well as the aging time of the entry.

The aging timer works as follows:

- If the user does not initiate authentication when the aging timer expires, the device deletes the temporary entry.
- If the user passes authentication before the aging timer expires, the device delete the aging timer and records online information for the Web authentication user.
- If the user fails authentication before the aging timer expires and an Auth-Fail VLAN is specified for Web authentication, the device binds the MAC address of the user to the Auth-fail VLAN and reset the aging timer. If the user still fails authentication when the aging timer expires, the device deletes the temporary entry for the user.

Restrictions and guidelines

As a best practice, change the aging timer to a bigger value in the following cases:

- Web authentication users without access rights frequently send traffic in a short time. As a result, the access device continuously initiates the web authentication process, increasing the load on the device.
- When a user fails authentication, the user does not have enough time to obtain resources from the Auth-Fail VLAN, for example, it failed to download the virus patches.

Procedure

1. Enter system view.
system-view
2. Configure the aging timer for temporary MAC address entries.
web-auth timer temp-entry-aging *aging-time-value*
By default, the aging timer for temporary MAC address entries is 60 seconds.

Command reference

New command: web-auth timer temp-entry-aging

Use **web-auth timer temp-entry-aging** to configure the aging timer for temporary MAC address entries.

Use **undo web-auth timer temp-entry-aging** to restore the default.

Syntax

```
web-auth timer temp-entry-aging aging-time-value
```

```
undo web-auth timer temp-entry-aging
```

Default

The aging timer for temporary MAC address entries is 60 seconds.

Views

System view

Default command level

network-admin

Parameters

aging-time-value: Specifies the aging timer in seconds for temporary MAC address entries, in the range of 60 to 2147483647.

Usage guidelines

If Web authentication is enabled, the device generates a temporary MAC address entry when it detects traffic from a user for the first time. The entry records the MAC address, access interface, and VLAN ID of the user, as well as the aging time of the entry.

The aging timer works as follows:

- If the user does not initiate authentication when the aging timer expires, the device deletes the temporary entry.
- If the user passes authentication before the aging timer expires, the device delete the aging timer and records online information for the Web authentication user.
- If the user fails authentication before the aging timer expires and an Auth-Fail VLAN is specified for Web authentication, the device binds the MAC address of the user to the Auth-fail VLAN and reset the aging timer. If the user still fails authentication when the aging timer expires, the device deletes the temporary entry for the user.

As a best practice, change the aging timer to a bigger value in the following cases:

- Web authentication users without access rights frequently send traffic in a short time. As a result, the access device continuously initiates the web authentication process, increasing the load on the device.
- When a user fails authentication, the user does not have enough time to obtain resources from the Auth-Fail VLAN, for example, it failed to download the virus patches.

Examples

Set the aging timer for temporary MAC address entries to 500 seconds.

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

```
[Sysname] web-auth timer temp-entry-aging 500
```

Modified command: display web-auth

Syntax

```
display web-auth [ interface interface-type interface-number ]
```

Views

Any view

Change description

The command output added support for the **Temp entry aging time** field.

Display Web authentication configuration on GigabitEthernet 1/0/1.

```
<Sysname> display web-auth interface gigabitethernet 1/0/1
```

Global Web-auth parameters:

```
Temp entry aging time      : 500 s
HTTP proxy port numbers    : Not configured
HTTPS proxy port numbers   : Not configured
Total online web-auth users : 1
```

GigabitEthernet1/0/1 is link-up

```
Port role                  : Authenticator
Web-auth domain            : my-domain
Auth-Fail VLAN             : Not configured
Offline-detect             : Not configured
Max online users           : 1024
Web-auth enable            : Enabled
Host mode                  : Single-VLAN
Primary Web server         : aaa
Secondary Web server       : Not configured
```

Total online web-auth users: 1

Modified feature: Displaying the running configuration

Feature change description

As from this release, the **display current-configuration** command supports displaying all configuration information.

Command changes

Modified command: display current-configuration

Old syntax

```
display current-configuration [ [ configuration [ module-name ] | interface
[ interface-type [ interface-number ] ] ] | slot slot-number ]
```

New syntax

```
display current-configuration [ [ configuration [ module-name ] | interface
[ interface-type [ interface-number ] ] ] [ all ] | slot slot-number ]
```

Views

System view

Change description

The **all** keyword was added for the command to support displaying all configuration information.

Modified feature: Displaying the running configuration in current view

Feature change description

As from this release, the **display this** command supports displaying all configuration information in current view.

Command changes

Modified command: display this

Old syntax

```
display this
```

New syntax

```
display this [ all ]
```

Views

System view

Change description

The **all** keyword was added for the command to support displaying all configuration information in current view.

Modified feature: 802.1X periodic reauthentication timer

Feature change description

In this release, the maximum value for the 802.1X periodic reauthentication timer changed from 7200 to 86400.

Command changes

Modified command: dot1x timer reauth-period (system view)

Syntax

```
dot1x timer reauth-period reauth-period-value
```

Views

System view

Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in system view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in system view.

Modified command: dot1x timer reauth-period (interface view)

Syntax

```
dot1x timer reauth-period reauth-period-value
```

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in interface view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in interface view.

Modified feature: Periodic MAC reauthentication timer

Feature change description

In this release, the maximum value for the periodic MAC reauthentication timer changed from 7200 to 86400.

Command changes

Modified command: mac-authentication timer (system view)

Syntax

```
mac-authentication timer reauth-period reauth-period-value
```

Views

System view

Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in system view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in system view.

Modified command: mac-authentication timer (interface view)

Syntax

```
mac-authentication timer reauth-period reauth-period-value
```

Views

Layer 2 Ethernet interface view

Change description

Before modification: The value range for the periodic reauthentication timer is 60 to 7200 seconds in interface view.

After modification: The value range for the periodic reauthentication timer is 60 to 86400 seconds in interface view.

Modified feature: Configuring the padding mode and padding format for the Remote ID sub-option of Option 82

Feature change description

As from this release, you can configure the **hex** *remote-id* option when you configure the padding mode and padding format for the Remote ID sub-option of Option 82.

Command changes

Modified command: dhcp relay information remote-id

Old syntax

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

New syntax

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

Views

Interface view

Change description

Before modification: The **hex** *remote-id* option is not supported in this command.

After modification: The **hex** *remote-id* option is supported in this command.

Parameters

hex *remote-id*: Pads the Remote ID sub-option with a user-defined hexadecimal string of 2 to 256 characters. The number of characters in the string must be even.

Modified feature: Configuring gRPC collectors

Feature change description

As from this release, you can add collectors to a destination group by their domain names. When you specify collectors by their domain names, use the following restrictions and guidelines:

- You must configure DNS to make sure the device can translate the domain names of the collectors to IP addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

- To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device will push data to the first reachable IP address.

Command changes

New command: domain-name

Use **domain-name** to add the domain name of an IPv4 collector to a destination group.

Use **undo domain-name** to remove the domain name of an IPv4 collector from a destination group.

Syntax

```
domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]

undo domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
```

Default

A destination group does not contain IPv4 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

domain-name: Domain name mapped to the IPv4 address of a collector. It can be a case-insensitive string of 1 to 253 characters and can contain letters, digits, hyphens (-), and dots (.).

port *port-number*: Specifies the service port number on which the collector receives data. The value range is 1 to 65535 and the default is 50051. To have the collector receive data, make sure the specified service port number is the same as the one used on the collector.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the collector belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Make sure the specified VPN instance already exists. If the collector is on the public network, do not specify this option.

tls: Enables Transport Layer Security (TLS) to encrypt the gRPC connection between the device and the specified collector. The device will then use a root TLS certificate that came with it for encryption. By default, the gRPC connection between the device and a collector is unencrypted.

Usage guidelines

If you specify collectors by their domain names, you must configure DNS to make sure the device can translate the domain names of the collectors to IPv4 addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device will push data to the first reachable IP address.

To add multiple collectors, repeat this command.

A collector is uniquely identified by a three-tuple of domain name, port number, and VPN instance name. One collector must have a different domain name, port number, or VPN instance name than the other collectors.

If you execute this command multiple times to change the TLS enabling state for a collector, the most recent configuration takes effect.

A destination group can have a maximum of five collectors.

You can enable TLS encryption globally by executing the **grpc pki domain** command in system view or enable collector-specific TLS encryption by specifying the **tls** keyword when you specify the collector. For a collector, the setting in system view has higher priority than the collector-specific setting.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Add the IPv4 collector at **sample.com** to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] domain-name sample.com
```

Related commands

destination-group (subscription view)

subscription

display dns host (*Layer 3—IP Services Command Reference*)

New command: ipv6 domain-name

Use **ipv6 domain-name** to add the domain name of an IPv6 collector to a destination group.

Use **undo ipv6 domain-name** to remove the domain name of an IPv6 collector from a destination group.

Syntax

```
ipv6 domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
```

```
undo ipv6 domain-name domain-name [ port port-number ] [ vpn-instance vpn-instance-name ] [ tls ]
```

Default

A destination group does not contain IPv6 collectors.

Views

Destination group view

Predefined user roles

network-admin

Parameters

domain-name: Domain name mapped to the IPv6 address of a collector. It can be a case-insensitive string of 1 to 253 characters and can contain letters, digits, hyphens (-), and dots (.).

port *port-number*: Specifies the service port number on which the collector receives data. The value range is 1 to 65535 and the default is 50051. To have the collector receive data, make sure the specified service port number is the same as the one used on the collector.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the collector belongs. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31

characters. Make sure the specified VPN instance already exists. If the collector is on the public network, do not specify this option.

tls: Enables Transport Layer Security (TLS) to encrypt the gRPC connection between the device and the specified collector. The device will then use a root TLS certificate that came with it for encryption. By default, the gRPC connection between the device and a collector is unencrypted.

Usage guidelines

If you specify IPv6 collectors by their domain names, you must configure DNS to make sure the device can translate the domain names of the collectors to IPv6 addresses. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To view domain name and IP address mappings, use the **display dns host** command. If a domain name maps to multiple IP addresses, the device will push data to the first reachable IP address.

To add multiple collectors, repeat this command.

A collector is uniquely identified by a three-tuple of domain name, port number, and VPN instance name. One collector must have a different domain name, port number, or VPN instance name than the other collectors.

If you execute this command multiple times to change the TLS enabling state for a collector, the most recent configuration takes effect.

A destination group can have a maximum of five collectors.

You can enable TLS encryption globally by executing the **grpc pki domain** command in system view or enable collector-specific TLS encryption by specifying the **tls** keyword when you specify the collector. For a collector, the setting in system view has higher priority than the collector-specific setting.

To modify the collector configuration for a destination group that is already used by a subscription, you must remove the destination group from the subscription first.

Examples

Add the IPv6 collector at **sample.com** to destination group **collector1**.

```
<Sysname> system-view
[Sysname] telemetry
[Sysname-telemetry] destination-group collector1
[Sysname-telemetry-destination-group-collector1] ipv6 domain-name sample.com
```

Related commands

destination-group (subscription view)

subscription

display dns host (Layer 3—IP Services Command Reference)

Modified command: display grpc

Syntax

```
display grpc [ verbose ]
```

Views

Any view

Change description

Before modification: The output from this command contains the **Encoding** and **Telemetry data mode** field. However, the command output does not contain the **Domain name** field.

After modification: The **Domain name** field is available in the command output. The **Encoding** and **Telemetry data mode** fields are not available in the command output.

Modified feature: Displaying detailed information about 802.1X online users

Feature change description

As from this version, the **display dot1x connection** command can display the AAA authentication method used by each user when they come online.

Command changes

Modified command: display dot1x connection

Syntax

```
display dot1x connection [ open ] [ interface interface-type  
interface-number | slot slot-number | user-mac mac-address | user-name  
name-string ]
```

Views

Any view

Change description

The **AAA authentication method** field was added to the command output. The value for this field can be **Local**, **HWTACACS**, **RADIUS**, or **None**.

The following shows an example:

Display information about all 802.1X online users.

```
<Sysname> display dot1x connection
```

```
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```
User access state: Successful
```

```
Authentication domain: aaa
```

```
IPv4 address: 192.168.1.1
```

```
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
```

```
Authentication method: CHAP
```

```
AAA authentication method: Local
```

```
Initial VLAN: 1
```

```
Authorization untagged VLAN: 6
```

```
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33  
35 37 40 to 100
```

```
Authorization ACL number/name: 3001
```

```
Authorization dynamic ACL name: N/A
```

```
Authorization user profile: N/A
```

```
Authorization CAR: N/A
```

```
Authorization URL: N/A
```

Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s

Release 6337P01

This release has the following changes:

- New feature: Configuring SmartMC
- New feature: Configuring interface alarm functions
- New feature: Configuring Option 60 for DHCP requests
- New feature: Configuring the type of port ID TLVs advertised by LLDP
- New feature: Enabling displaying LLDP local information about all interfaces
- New feature: PoE forced power supply
- New feature: Interval at which the SNMP module examines the system configuration for changes
- New feature: Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users
- New feature: Automated IPv6 underlay network deployment for VCF fabric
- Modified feature: Setting the port status detection timer
- Modified feature: 802.1X EAD assistant
- Modified feature: Displaying information about online MAC authentication users
- Modified feature: L2PT for CFD

New feature: Configuring SmartMC

About SmartMC

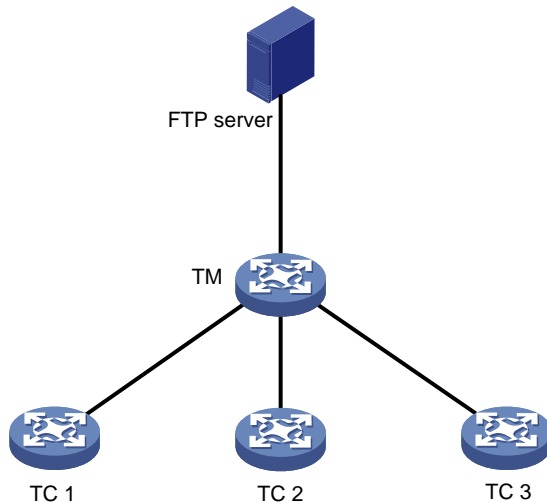
Smart Management Center (SmartMC) centrally manages and maintains dispersed network devices at network edges. In a SmartMC network, only one device acts as the commander and the remaining devices all act as members. SmartMC provides the following features for you to manage the members from the commander:

- Configuration file backup and download.
- Software upgrade.
- Configuration deployment.
- Faulty member replacement.

SmartMC network framework

Figure 1 shows the basic framework of a SmartMC network.

Figure 1 SmartMC network framework



The SmartMC network contains the following elements:

- **Commander**—Also called topology master (TM), which manages all members in the SmartMC network.
- **Member**—Also called topology client (TC), which is managed by the commander.
- **File server**—Stores startup software images and configuration files for the commander and members.

SmartMC network establishment

A SmartMC network can be established automatically or manually. In an automatically established SmartMC network, the commander obtains member information through NETCONF sessions to form the network topology. The member information includes port information, LLDP neighbor information, STP information, device type, and software version. In a manually established SmartMC network, the commander obtains member's LLDP neighbor information through NETCONF sessions and member's hardware information through SNMP Get operations.

Automatic SmartMC network establishment

The commander and members use the following procedure to establish a SmartMC network:

1. After SmartMC is enabled, the commander broadcasts a SmartMC packet at an interval of 15 seconds to detect members in the network. The SmartMC packet contains information of the commander, such as its bridge MAC address and the IP address of VLAN-interface 1.
2. When a member receives the packet, it records the commander information, and returns a response packet to the commander. The response packet contains information of the member, such as its bridge MAC address and the IP address of VLAN-interface 1.
3. When the commander receives the response packet, it initiates a NETCONF session to the member with the default username **admin** and the default password **admin**. The commander then obtains detailed information about the member through the session, including port information, LLDP neighbor information, STP information, device type, and software version.
4. The commander establishes a connection to the member for tracking the liveliness of the member, and adds the member to the SmartMC network.
5. Based on the LLDP neighbor information obtained from all members, the commander forms a SmartMC topology.

After the SmartMC network is established, the commander and members check for the existence of each other by exchanging SmartMC packets.

- When a member receives a SmartMC broadcast packet from the commander, it compares the bridge MAC address in the packet with the recorded bridge MAC address. If the two bridge MAC addresses are the same, the member returns a response packet to the commander. If the member does not receive a broadcast packet from the commander within the time limit, the member determines that the commander does not exist in the network anymore. Then, the member clears the commander information. The time limit is a random value in the range of 60 to 120 seconds.
- When the commander receives a response packet from a member, it compares the bridge MAC address in the packet with the recorded bridge MAC address. If the two bridge MAC addresses are the same, the commander determines that the member still exists in the network. If the commander does not receive a response packet from a member within 150 seconds, the commander determines that the member is offline. Then, the commander sets the status of the member to offline.

Manual SmartMC network establishment

You can log in to the Web interface of the commander, and enter the IP address, username, and password of the members to manually add them to the network. The members can join the network without exchanging SmartMC packets with the commander. For more information, see *Comware 7 Web-Based Products User Guide*.

After you specify the information of a member on the commander, the commander performs the following operations to add the member to the network:

- Verify that the member can be accessed through Telnet.
- Obtain basic member information, including LLDP neighbor information through NETCONF.
- Obtain hardware information through SNMP Get operations.

SmartMC features

Bulk configuration deployment for members

This feature allows you to deploy multiple command lines to members from the commander, eliminating the need to log in to members and configure the command one by one.

The procedure for bulk configuration deployment is as follows:

1. The commander acts as a Telnet client and establishes Telnet connections to the members.
2. The commander deploys a batch file to the members through Telnet connections. The batch file is created on the commander and contains command lines to be deployed.
3. The members run the command lines in the file.

Bulk configuration deployment for ports connecting APs and IP phones

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration.

When the commander first detects the association of an AP or IP phone on a port through LLDP, it deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

If the AP or IP phone disconnects from the port, the configurations on the port remain. When a new device comes online from the port, configurations used by the port depend on the new device type.

- If the new device is an AP or IP phone and has the same type as the disconnected device, the configurations on the port remain unchanged.
- If the new device is an AP or IP phone but has a different type as the disconnected device, the commander deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.
- If the new device is neither an AP nor an IP phone, the configurations on the port remain unchanged.

To disable the commander from deploying a batch file to ports, remove the specified batch file or execute the `undo smartmc batch-file-apply enable` command to disable batch file deployment.

Configuration file backup

You can use the following methods to back up the next-startup configuration file on the commander and members:

- **Automatic backup**—Enable this feature for the commander and all members in the network to immediately perform a backup. After that, the commander and members back up the configuration file at a user-specified interval.
- **Manual backup**—Manually trigger a backup on the commander or the specified members or SmartMC groups.

To back up the configuration file on a member, the commander instructs the member by unicasting a SmartMC packet to them. When a member receives the packet, it saves the running configuration to the next-startup configuration file and uploads the file to the file server.

Startup software and configuration file upgrade

This feature enables users to upgrade startup software and the configuration file of member devices from the commander.

Before upgrade, you must upload the upgrade files from the commander to the file server and specify the upgrade files on the file server for the members to download.

The procedure for startup software and configuration file upgrade is as follows:

1. The commander instructs the members (or SmartMC group) to download the upgrade files from the file server.
2. The members download the upgrade files from the file server.
3. The members upgrade the startup software and configuration file as follows:
 - **Startup software upgrade**—Uses the boot loader method to perform the software upgrade. The members might be restarted during the upgrade process.
 - **Configuration file upgrade**—Replaces the current configuration file with the upgrade configuration file. The members will not be restarted during the upgrade process.

Faulty member replacement

You can use the following methods to replace a faulty member:

- **Automatic replacement**—Enables the commander to record the positions of all members in the topology for replacement. When the commander discovers that the new member has physically replaced the faulty member, it compares the new member with the faulty one. The commander performs a replacement if the following requirements are met:
 - The new member is deployed at the same topological position as the faulty one.
 - The models of the new member and faulty member are the same.

The commander then instructs the new member to download the configuration file of the faulty member from the file server. After downloading the configuration file, the new member runs the configuration file to complete the replacement.

- **Manual replacement**—After the faulty member is physically replaced, you manually trigger a configuration replacement. The new member will download the configuration file of the faulty member from the file server and run the file to complete the replacement.

Outgoing interface for a SmartMC network

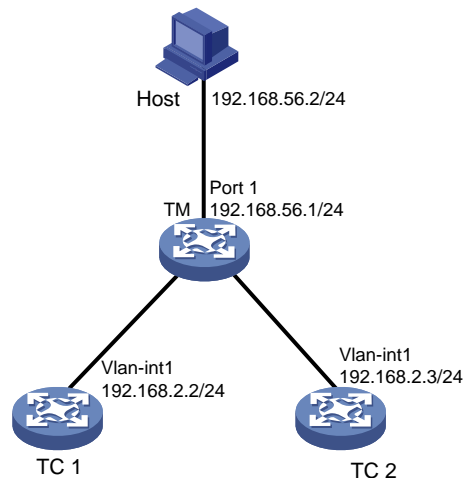
The outgoing interface feature allows hosts connecting to an outgoing interface to access all the members in a SmartMC network. You can configure multiple outgoing interfaces for a SmartMC network.

As shown in [Figure 2](#), the host is connected to port 1 on the TM and TC 1 and TC 2 are in a different network segment than the host. The host can access the Web interface of the TM but cannot access the Web interface of any member.

If port 1 on the TM is configured as the outgoing interface, the system mirrors the IP address of each member to a new address. The new address contains the IP address of the outgoing interface and the port number assigned by the commander to the member in the format of *IP address:Port number*. This enables the host to access the Web interfaces of members from the Web interface of the TM.

To access the Web interface of a member, enter the Web interface of the commander, and click **Visibility** from the navigation pane. Then, click the **Topology** tab, select the target member, and click **Login to Web interface**.

Figure 2 SmartMC network



Automatic link aggregation

Automatic link aggregation automatically bundles multiple physical Ethernet links between two members into one logical link, called an aggregate link. This feature provides increased link bandwidth and improved link reliability.

NOTE:

- Automatic link aggregation cannot be performed between the commander and a member, or between a member and a device outside the SmartMC network. You can aggregate the links between the commander and a member manually. For more information about manual link aggregation, see Ethernet link aggregation in *Layer 2—LAN Switching Configuration Guide*.
 - If a member enabled with automatic link aggregation joins a SmartMC network whose commander is disabled with the aggregation feature, the feature will be disabled for the member as well. This might affect service traffic forwarding on the member.
-

VLAN creation for members

To simplify configuration and management, you can create a VLAN for members. Then, all access ports on a member that are not connected to other members or the commander are assigned to the VLAN.

If a member has access ports that are connected to offline devices, you must remove the offline devices before creating a VLAN for the member.

The VLAN creation fails for a member if one or more access ports cannot be assigned to the VLAN. If the VLAN creation fails, the VLAN memberships for the access ports are restored to the state before the VLAN was created.

The failure to create a VLAN for a member does not affect the VLAN creation for other members.

Resource monitoring

Resource monitoring allows you to view resource usage, memory usage, temperature information, and packet dropping information of commanders and members on the commander.

You can view the usage and temperature information on the commander, and view packet dropping information from the **SmartMC > Intelligent O&M > Resource monitoring** page of the commander's Web interface.

Restrictions: Hardware compatibility with SmartMC

The HPE 5140 EI switch series cannot act as the commander. The switches only support SmartMC members.

Restrictions and guidelines: SmartMC configuration

You need to enable SmartMC on both the commander and members and perform all the other tasks only on the commander.

The following features take effect only on members added to the SmartMC network automatically:

- Configuration file backup.
- Faulty member replacement.
- Startup software and configuration file upgrade.
- Automatic link aggregation.

A SmartMC network is established in VLAN 1. For the network to work correctly, do not configure security settings in VLAN 1.

SmartMC tasks at a glance

To configure SmartMC, perform the following tasks:

1. [Enabling SmartMC](#)

2. [Setting the file server information](#)

This task is required for configuring automatic configuration file backup, replacing faulty members, and upgrading the startup software and configuration file on members.

3. (Optional.) [Configuring an outgoing interface for the SmartMC network](#)

4. (Optional.) [Enabling automatic Ethernet link aggregation](#)

5. (Optional.) [Modifying the password of the default user for members](#)

6. [Creating a SmartMC group](#)

This task is required for upgrading the startup software and configuration file on members and deploying a batch file to a SmartMC group.

7. (Optional.) Deploying and managing configuration

- [Creating a VLAN for members](#)
- [Deploying a batch file to members](#)
- [Configuring a batch file for ports connecting APs or IP phones](#)
- [Backing up configuration files](#)

8. (Optional.) Monitoring and maintaining the SmartMC network

- [Configuring resource monitoring](#)
- [Upgrading the startup software and configuration file on members](#)
- [Managing the network topology](#)
- [Replacing faulty members](#)

Prerequisites for SmartMC

Before you configure SmartMC, perform the following tasks on the commander and members:

- Enable the Telnet service, and configure scheme authentication for VTY user lines. For information about Telnet service and VTY user lines, see CLI login configuration in *Fundamentals Configuration Guide*.
- Configure a local user.
 - Specify the username and password.
 - On the commander, the username and password must be the same as the username and password configured by using the **smartmc tm username username password { cipher | simple } string enable** command.
 - On a member, set both the username and password to **admin**, and execute the **password-control length 4 password-control composition type-number 1 type-length 1**, and **undo password-control complexity user-name check** commands to lower the password complexity requirements.

This is because SmartMC requires that the commander use username **admin** and password **admin** to communicate with members, which does not meet the default password complexity requirements. For more information about these commands, see password control commands in *Security Command Reference*.

After the SmartMC network is established, you can increase the password complexity requirements and use the **smartmc tc password** command to modify the username and password.
 - Specify the Telnet, HTTP, and HTTPS services for the user.
 - Set the RBAC role of the local user to network-admin.

For information about local users, see AAA configuration in *Security Configuration Guide*. For information about user roles, see RBAC configuration in *Fundamentals Configuration Guide*.

- Enable NETCONF over SOAP over HTTP. For information about NETCONF over SOAP, see NETCONF configuration in *Network Management and Monitoring Configuration Guide*.
- Enable LLDP globally. For information about LLDP, see *Layer 2—LAN Switching Configuration Guide*.
- To manage the commander and members through a Web interface, you must enable the HTTP and HTTPS services, and set the service type to HTTP and HTTPS for the local user. For information about Web login, HTTP, and HTTPS, see *Fundamentals Configuration Guide*.
- To manually establish a SmartMC network, you must configure the **snmp-agent community read public** and **snmp-agent sys-info version v2c** commands on the members. For information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Enabling SmartMC

About SmartMC

Enable this feature on both the commander and members to enable management of members from the commander.

Restrictions and guidelines

A SmartMC network must have one and only one commander.

If you change the role of the commander to member or disable SmartMC on the commander, all SmartMC settings in its running configuration will be cleared.

SmartMC fails to be enabled if ACL resources are insufficient. If ACL resources are insufficient, use the **undo acl** command to delete unnecessary ACLs and then enable SmartMC. You can execute

the **display acl** command to view ACL configuration and match statistics. For more information about ACLs, see *ACL and QoS Configuration Guide*.

SmartMC fails to be enabled if ports 80 and 443 have been used.

If you execute the **smartmc enable** command multiple times, the most recent configuration takes effect. You can execute the command to change the device role or the password.

Procedure

1. Enter system view.
system-view
2. Enable SmartMC and set the device role.
smartmc { tc | tm username *username* password { cipher | simple } string } enable
By default, SmartMC is disabled.

Setting the file server information

About files stored on the file server

In a SmartMC network, a file server is used to store the following files:

- Upgrade startup software files and upgrade configuration file for members.
- Backup configuration files of the commander and members.

For information about FTP servers, see configuring FTP in *Fundamentals Configuration Guide*. For information about SFTP servers, see configuring SSH in *Security Configuration Guide*.

Restrictions and guidelines

You can use the following methods to specify a file server:

- Specify the IP address of a file server.
- Specify the IP address of the commander. The commander will act as a file server.

To configure the commander to act as a file server, make sure the commander has enough storage space for storing the files required by members.

To use an independent file server, connect the file server to the commander instead of the members as a best practice. The file server uses VLAN 1 to communicate with the SmartMC network. If you connect the file server to members, creating a VLAN for members will assign member interfaces connecting to the file server to the created VLAN, causing file server disconnection. For more information about member VLAN creation, see "[Creating a VLAN for members](#)."

Procedure

1. Enter system view.
system-view
2. Set the file server information.
smartmc { ftp-server | sftp-server } { ipv4-address | ipv6 *ipv6-address* } [port *port*] [vpn-instance *vpn-instance-name*] [directory *directory*] username *username* password { cipher | simple } *string*
By default, no file server information is set.

Configuring an outgoing interface for the SmartMC network

Restrictions and guidelines

VLAN interface 1 cannot be used as an outgoing interface, because the SmartMC network is established in VLAN 1.

Procedure

1. Enter system view.
system-view
2. Enter VLAN interface view.
interface vlan *interface-number*
3. Configure the interface as an outgoing interface.
smartmc outbound

By default, no interface is used as an outgoing interface.

Enabling automatic Ethernet link aggregation

Restrictions and guidelines

Enabling or disabling automatic link aggregation might cause network flapping, and the members might go offline for a short period of time.

Procedure

1. Enter system view.
system-view
2. Enable automatic Ethernet link aggregation.
smartmc auto-link-aggregation enable

By default, automatic Ethernet link aggregation is disabled.

Modifying the password of the default user for members

About modifying the password of the default user for members

During SmartMC network establishment, the commander uses the default username and password to establish NETCONF sessions to members automatically added to the network. The default username and password of the members for NETCONF session establishment are **admin** and **admin**.

To enhance security, you can perform this task to change the password for the default user **admin** of the members after the commander adds the members to the network.

Restrictions and guidelines

Do not modify the password for members that are manually added to the SmartMC network. If you modify the password for a manually added member, you will not be able to manage that member from the commander.

You can use the **display smartmc tc verbose** command to identify the method used to add the members.

Procedure

1. Enter system view.
system-view

2. Modify the password of the default user for members.

```
smartmc tc password [cipher] string
```

Creating a SmartMC group

About SmartMC groups

This feature allows you to create a SmartMC group on the commander and add members to the group. When you perform the following operations, you can specify a SmartMC group to apply the operations to all members in the group:

- Startup software upgrade.
- Configuration file upgrade.
- Configuration deployment.

Procedure

1. Enter system view.

```
system-view
```

2. Create a SmartMC group and enter its view.

```
smartmc group group-name
```

3. (Optional.) Display predefined device types.

```
match device-type ?
```

If the device type of the members is not predefined on the commander, you must manually add the device type to the commander. This enables members of an undefined type to join a SmartMC group created on the commander.

4. Set a match criterion.

```
match { device-type device-type | ip-address ip-address  
{ ip-mask-length | ip-mask } | mac-address mac-address mac-mask-length }
```

By default, no match criterion is set.

5. If the device type of the members is not predefined on the commander, perform the following tasks to manually define the device type on the commander:

- a. Return to system view.

```
quit
```

- b. Define a device type on the commander.

```
smartmc tc sysoid sysoid device-type device-type
```

To obtain the SYSOID of a member, execute the **display smartmc tc verbose** command.

You cannot define a predefined member type as another type.

Creating a VLAN for members

Restrictions and guidelines

If you perform this task multiple times to create a VLAN for members, the most recent configuration takes effect.

Procedure

1. Enter system view.

```
system-view
```

2. Creating a VLAN for members and assign access ports on the members to the VLAN.

```
smartmc vlan vlan-id { group group-name-list | tc tc-id-list }
```

Deploying a batch file to members

1. Execute the following command in user view to create a batch file and edit the command lines to be deployed to members.

```
create batch-file cmd-filename
```

Each command occupies a line in the batch file. When you finish editing, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

2. Enter system view.

```
system-view
```

3. Deploy the batch file to a list of members or SmartMC groups.

```
smartmc batch-file cmd-filename deploy { group group-name-list | tc tc-id-list }
```

Configuring a batch file for ports connecting APs or IP phones

Restrictions and guidelines

All commands in the batch file must be commands used in interface view.

The size of the batch file cannot exceed 8190 characters.

Make sure the file name is correct when specifying the batch file because the system does not verify whether the file name is correct. After specifying the batch file, do not delete the file or rename the file.

Procedure

1. (Optional.) Execute the following command in user view to create a batch file and edit the command lines to be deployed to members.

```
create batch-file cmd-filename
```

Each command occupies a line in the batch file. When you finish editing, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

2. Enter system view.

```
system-view
```

3. Specify the batch file for ports connecting APs or IP phones.

```
smartmc batch-file batch-file-name apply { ap | phone }
```

4. (Optional.) Disable batch file deployment.

```
undo smartmc batch-file-apply enable
```

By default, batch file deployment is enabled.

Backing up configuration files

About backing up configuration files

Perform this task to back up the configuration file of the commander or the specified members. Configuration files automatically backed up to the file server are named in the format of *device bridge MAC address_backup.cfg*.

Restrictions and guidelines

When you change the commander in the SmartMC network, make sure the backup configuration file of the original commander on the file server is deleted. If the file still exists, the new commander might download the file and run the settings. This will cause a conflict in the network.

The maximum number of members that can perform automatic configuration at the same time is limited by the performance of the file server. If automatic configuration backup fails, set the maximum number of members to a smaller value.

Prerequisites

Before performing this task, you must set the file server information (see "[Setting the file server information](#)").

Procedure

1. Enter system view.

```
system-view
```

2. Set the maximum number of members that can perform configuration file backup at the same time.

```
smartmc backup configuration max-number max-number
```

By default, a maximum of five members can perform automatic configuration backup at the same time.

3. Back up configuration files.

Choose one option as needed:

- o Enable automatic configuration file backup and set the backup interval.

```
smartmc backup startup-configuration interval interval-time
```

By default, automatic configuration file backup is disabled.

- o Manually back up the configuration file on members.

```
smartmc backup configuration { group group-name-list | tc
[ tc-id-list ] }
```

TC ID 0 represents the commander.

Configuring resource monitoring

1. Enter system view.

```
system-view
```

2. Set the interval for the commander to obtain resource monitoring information.

```
smartmc resource-monitor interval interval
```

The default setting is 1 minute.

3. Set the aging time for resource monitoring information.

```
smartmc resource-monitor max-age max-age
```

The default setting is 24 hours.

4. Enable resource monitoring.

```
smartmc resource-monitor [ cpu | memory | packet-drop | temperature ] *
[ group group-name-list | tc { tc-id-list | mac-address mac-address } | tm ]
```

By default, resource monitoring is disabled.

If you do not specify a resource type, this command enables resource monitoring for all resource types.

If you do not specify a device to monitor (member or commander), this command enables resource monitoring on the commander and all members.

Upgrading the startup software and configuration file on members

About upgrading the startup software and configuration file on members

You can use the following methods to upgrade the startup software and configuration file on members:

- Schedule an upgrade by specifying an upgrade time or upgrade delay.
- Upgrade immediately by not specifying an upgrade time or upgrade delay.

Restrictions and guidelines for startup software and configuration file upgrade

A member can perform only one upgrade task at a time.

An immediate upgrade cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

Prerequisites

Before performing this task, you must set the file server information (see "[Setting the file server information](#)").

Upgrading the startup software and configuration file on members

Upgrading the startup software and configuration file in one step

1. Enter system view.
system-view
2. Upgrade the startup software on members in one step.
smartmc upgrade boot-loader tc { *tc-id-list* { **boot** *boot-filename* **system** *system-filename* | **file** *ipe-filename* } }&<1-40> [**delay** *delay-time* | **time** *in-time*]

CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

3. Upgrade the configuration file on members in one step.
smartmc upgrade startup-configuration tc { *tc-id-list* *cfg-filename* }&<1-40> [**delay** *delay-time* | **time** *in-time*]

CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

Configuring startup software and configuration file upgrade step by step

1. Enter system view.
system-view
2. Configure startup software upgrade for members step by step:
 - a. Specify the upgrade startup software files.

```
smartmc tc tc-id boot-loader { ipe-filename | boot boot-filename system system-filename }
```

- b. Upgrade the startup software on members.

```
smartmc upgrade boot-loader tc tc-id-list
```

△ CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

3. Configure configuration file upgrade for members step by step:

- a. Specify the upgrade configuration file.

```
smartmc tc tc-id startup-configuration cfg-filename
```

- b. Upgrade the configuration file on members.

```
smartmc upgrade startup-configuration tc tc-id-list
```

△ CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

Upgrading the startup software and configuration file on all members in SmartMC groups

Upgrading the startup software and configuration file in one step

1. Enter system view.

```
system-view
```

2. Upgrade the startup software on all members in SmartMC groups in one step.

```
smartmc upgrade boot-loader group { group-name-list [ boot boot-filename system system-filename | file ipe-filename ] }&<1-40>  
[ delay minutes | time in-time ]
```

△ CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

3. Upgrade the configuration file on all members in SmartMC groups in one step.

```
smartmc upgrade startup-configuration group { group-name-list file cfg-filename }&<1-40> [ delay minutes | time in-time ]
```

△ CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

Configuring startup software and configuration file upgrade step by step

1. Enter system view.

```
system-view
```

2. Enter SmartMC group view.

smartmc group *group-name*

3. Specify the upgrade startup software files for the SmartMC group.

boot-loader file { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

By default, no upgrade startup software files are specified for a SmartMC group.

4. Specify the upgrade configuration file for the SmartMC group.

startup-configuration *cfgfile*

By default, no upgrade configuration file is specified for a SmartMC group.

5. Return to system view.

quit

6. Upgrade the startup software and configuration file on all members in the SmartMC group.

Choose one option as needed:

- Upgrade the startup software.

smartmc upgrade boot-loader group *group-name-list* [**delay** *minutes* | **time** *in-time*]

△ CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

- Upgrade the configuration file.

smartmc upgrade startup-configuration group *group-name-list* [**delay** *minutes* | **time** *in-time*]

△ CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

Managing the network topology

Refreshing the network topology

About refreshing the network topology

You can use the following methods to refresh the network topology:

- **Automatic topology refresh**—Specify the refresh interval to allow the commander to refresh the network topology periodically.
- **Manual topology refresh**—Execute the **smartmc topology-refresh** command to manually refresh the network topology.

Restrictions and guidelines

The topology refresh time depends on the number of members in the network.

Procedure

Choose one option as needed:

- Manually refresh the network topology in any view.

smartmc topology-refresh

- Configure automatic network topology refresh.
 - a. Enter system view.
`system-view`
 - b. Set the automatic topology refresh interval.
`smartmc topology-refresh interval interval`
By default, the automatic topology refresh interval is 60 seconds.

Saving the network topology

About saving the network topology

This task allows you to save the current network topology to the **topology.db** file in the flash memory. After the commander reboots, it uses the **topology.db** file to restore the network topology.

Procedure

1. Enter system view.
`system-view`
2. Save the network topology.
`smartmc topology-save`

Replacing faulty members

Restrictions and guidelines

Make sure the new member for replacement and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Make sure the new member has a different member ID than all the members in the SmartMC network, including offline members. Faulty members are considered offline.

To automatically replace a faulty member, first enable automatic replacement, and then install the new member at the location where the faulty member was installed and connect all cables.

To manually replace a faulty member, first install the new member at the location where the faulty member was installed, connect all cables, and then execute the manual replacement command.

Prerequisites

Before you replace a faulty member, set the file server information (see "[Setting the file server information](#)").

Procedure

1. Enter system view.
`system-view`
2. Replace faulty members.
Choose one option as needed:
 - Enable automatic faulty member replacement.
`smartmc auto-replace enable`
By default, automatic faulty member replacement is disabled.
 - Manually replace a faulty member.
`smartmc replace tc tc-id1 faulty-tc tc-id2`

Display and maintenance commands for SmartMC

Execute **display** commands in any view.

Task	Command
Display the backup status on members.	display smartmc backup configuration status
Display the batch file execution results.	display smartmc batch-file status [ap last <i>number</i> / phone]
Display SmartMC configuration.	display smartmc configuration
Display connections between the devices in the SmartMC network.	display smartmc device-link
Display SmartMC group information.	display smartmc group [<i>group-name</i>] [verbose]
Display the faulty member replacement status.	display smartmc replace status
Display resource monitoring information.	display smartmc resource-monitor [cpu memory temperature] * [tc <i>tc-id</i> tm]
Display resource monitoring configuration.	display smartmc resource-monitor configuration
Display member information.	display smartmc tc [<i>tc-id</i>][verbose]
Display log information in the log buffer on a member.	display smartmc tc <i>tc-id</i> log buffer [module <i>module-name</i> [mnemonic <i>mnemonic-value</i>]]
Display restart log information for a member.	display smartmc tc <i>tc-id</i> log restart
Display VLAN creation results for members.	display smartmc vlan
Display member upgrade status.	display smartmc upgrade status

SmartMC configuration examples

Example: Configuring SmartMC

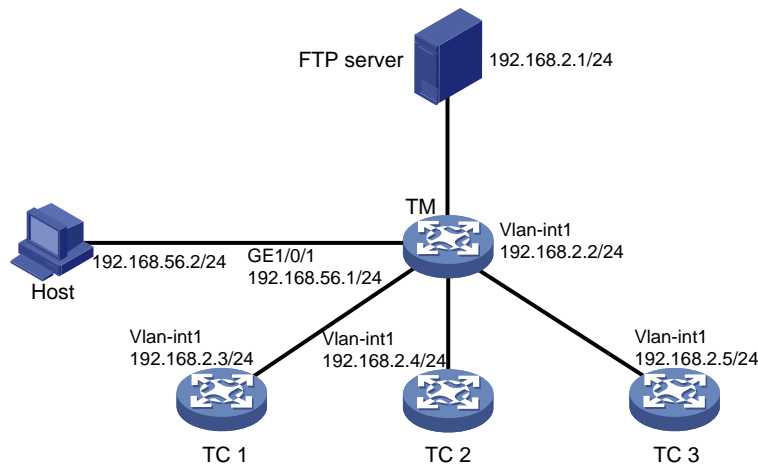
Network configuration

As shown in [Figure 3](#), member 1, member 2, and member 3 belong to the same device type: S5130S-HI series. The IP address of the FTP server is 192.168.2.1. The FTP username is **admin** and the FTP password is **hello12345**.

Perform the following tasks to establish a SmartMC network and upgrade the configuration file on the members:

1. Configure the commander and members to automatically establish a SmartMC network.
2. Configure interface GigabitEthernet 1/0/1 as the outgoing interface for the SmartMC network.
3. Create a SmartMC group and add the members to the group.
4. Upgrade the configuration file on all members in the SmartMC group.
5. Save configuration file **startup.cfg** on the FTP server.

Figure 3 Network diagram



Procedure

1. Configure TC 1:

Configure VLAN-interface 1.

```

<TC1> system-view
[TC1] interface vlan-interface 1
[TC1-Vlan-interface1] ip address 192.168.2.3 24
[TC1-Vlan-interface1] quit

```

Enable HTTP and HTTPS.

```

[TC1] ip http enable
[TC1] ip https enable

```

Enable the Telnet service.

```

[TC1] telnet server enable

```

Enable NETCONF over SOAP over HTTP.

```

[TC1] netconf soap http enable

```

Enable LLDP globally.

```

[TC1] lldp global enable

```

Create a user named **admin**.

```

[TC1] local-user admin

```

Lower password complexity requirements. For more information about these commands, see password control commands in *Security Command Reference*.

```

[TC1-luser-manage-admin] password-control length 4
[TC1-luser-manage-admin] password-control composition type-number 1 type-length 1
[TC1-luser-manage-admin] undo password-control complexity user-name check

```

Set the password to **admin**, add the **telnet**, **http**, and **https** service types, and authorize the user to use the **network-admin** user role.

```

[TC1-luser-manage-admin] password simple admin
[TC1-luser-manage-admin] service-type telnet http https
[TC1-luser-manage-admin] authorization-attribute user-role network-admin
[TC1-luser-manage-admin] quit

```

Set scheme authentication for VTY user lines 0 to 63.

```

[TC1] line vty 0 63
[TC1-line-vty0-63] authentication-mode scheme

```

```

[TC1-line-vty0-63] quit
# Enable SmartMC and set the device role to tc.
[TC1] smartmc tc enable
2. Configure TC 2 and TC 3 in the same way TC 1 is configured. (Details not shown.)
3. Configure the TM:
# Configure GigabitEthernet 1/0/1.
<TM> system-view
[TM] interface gigabitethernet 1/0/1
[TM-GigabitEthernet1/0/1] port link-mode route
[TM-GigabitEthernet1/0/1] ip address 192.168.52.2 24
[TM-GigabitEthernet1/0/1] quit
# Configure VLAN-interface 1.
[TM] interface vlan-interface 1
[TM-Vlan-interface1] ip address 192.168.2.2 24
[TM-Vlan-interface1] quit
# Enable HTTP and HTTPS.
[TM] ip http enable
[TM] ip https enable
# Enable the Telnet service.
[TM] telnet server enable
# Enable NETCONF over SOAP over HTTP.
[TM] netconf soap http enable
# Enable LLDP globally.
[TM] lldp global enable
# Create a user. Set the username to admin and the password to hello12345, add the telnet,
http, and https service types, and authorize the user to use the network-admin user role.
[TM] local-user admin
[TM-luser-manage-admin] password simple hello12345
[TM-luser-manage-admin] service-type telnet http https
[TM-luser-manage-admin] authorization-attribute user-role network-admin
[TM-luser-manage-admin] quit
# Set scheme authentication for VTY user lines 0 to 63.
[TM] line vty 0 63
[TM-line-vty0-63] authentication-mode scheme
[TM-line-vty0-63] quit
# Enable SmartMC, set the device role to commander, and set the username to admin and the
password (plaintext) to hello12345.
[TM] smartmc tm username admin password simple hello12345 enable
# Specify GigabitEthernet 1/0/1 as the outgoing interface.
[TM] interface gigabitethernet 1/0/1
[TM-GigabitEthernet1/0/1] smartmc outbound
[TM-GigabitEthernet1/0/1] quit
# Set the FTP server IP address, username, and plaintext password to 192.168.2.1, admin,
and hello12345, respectively.
[TM] smartmc ftp-server 192.168.2.1 username admin password simple hello12345
# Create SmartMC group S1 and enter its view.
[TM] smartmc group S1

```

Create an IP address match criterion to add all members in the specified network segment to SmartMC group **S1**.

```
[TM-smartmc-group-S1] match ip-address 192.168.2.0 24
```

Specify the upgrade configuration file **startup.cfg** for SmartMC group **S1**.

```
[TM-smartmc-group-S1] startup-configuration startup.cfg
```

```
[TM-smartmc-group-S1] quit
```

Upgrade the configuration file on all members in SmartMC group **S1**.

```
[TM] smartmc upgrade startup-configuration group S1 file startup.cfg
```

Verifying the configuration

Display brief information about all members after the SmartMC network is established.

```
[TM] display smartmc tc
```

TCID	DeviceType	Sysname	IpAddress	MacAddress	Status	Version
1	S5130S-HI	TC1	192.168.2.3	201c-e7c3-0300	Normal	COMWAREV700R001
2	S5130S-HI	TC2	192.168.2.4	201c-e7c3-0301	Normal	COMWAREV700R001
3	S5130S-HI	TC3	192.168.2.5	201c-e7c3-0302	Normal	COMWAREV700R001

Display the configuration file upgrade status on the members.

```
<TM> display smartmc upgrade status
```

ID	IpAddress	MacAddress	Status	UpdateTime	UpdateFile
1	192.168.2.3	201c-e7c3-0300	Finished	Immediately	startup.cfg
2	192.168.2.4	201c-e7c3-0301	Finished	Immediately	startup.cfg
3	192.168.2.5	201c-e7c3-0302	Finished	Immediately	startup.cfg

Command reference

boot-loader file

Use **boot-loader file** to specify the upgrade startup software files for a SmartMC group.

Use **undo boot-loader** to restore the default.

Syntax

```
boot-loader file { ipe-filename | boot boot-filename system  
system-filename }
```

```
undo boot-loader
```

Default

No upgrade startup software files are specified for a SmartMC group.

Views

SmartMC group view

Predefined user roles

network-admin

Parameters

ipe-filename: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

boot *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

system *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Specify IPE software file device.ipe for SmartMC group testgroup.
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup] boot-loader file device.ipe
```

Related commands

```
smartmc group
smartmc upgrade boot-loader
```

create batch-file

Use **create batch-file** to create a batch file.

Syntax

```
create batch-file batch-file-name
```

Default

No batch files exist.

Views

User view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies the name of the batch file, a case-insensitive string of 1 to 255 characters. If you do not specify a file extension when specifying a file name, the default extension **.cmdset** is used.

Usage guidelines

After executing this command, you will enter the batch edit mode. In this mode, each command occupies a line. When you finish editing all command lines, enter a percent sign (%) to return to user view.

Make sure the command lines that you enter are correct because the system does not verify whether the command lines are correct.

Examples

```
# Create a batch file named test.cmdset, and enter the command lines for specifying the device name as Sysname and enabling Telnet.
<Sysname> create batch-file test.cmdset
Begin to edit batch commands, and quit with the character '%'.
system-view
sysname Sysname
telnet server enable%
<Sysname>
```

Related commands

```
display smartmc batch-file status
smartmc batch-file deploy
```

display smartmc backup configuration status

Use `display smartmc backup configuration status` to display the backup status on members.

Syntax

```
display smartmc backup configuration status
```

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command displays the status of the ongoing backup task or the most recent backup task if the member is not performing backup.

Examples

Display the backup status on members.

```
<Sysname> display smartmc backup configuration status
```

ID	IpAddress	MacAddress	Status	Time
1	192.168.56.30	08d2-38ff-0300	Finished	2017-04-05 11:30:35
2	192.168.56.40	62d2-c21c-0400	Finished	2017-04-05 11:30:40

Table 1 Command output

Field	Description
ID	ID of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Backup status: <ul style="list-style-type: none">• Waiting—The member is waiting for configuration backup.• Processing—The member is backing up the configuration.• Finished—The member has finished backing up the configuration.• Timeout—Configuration backup times out.• Failed—The member failed to back up the configuration.
Time	Time when the member finished backing up the configuration. If the member has not finished backing up the configuration, this field displays a hyphen (-).

Related commands

```
smartmc backup configuration
smartmc backup configuration interval
smartmc backup configuration max-number
```

display smartmc batch-file status

Use **display smartmc batch-file status** to display the batch file deployment result.

Syntax

```
display smartmc batch-file status [ ap | last number | phone ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

ap: Displays the result of the most recent batch file deployment for ports connected to APs.

last number: Specifies a batch file deployment (performed by using the **smartmc batch-file deploy** command) by its number counting from the most recent batch file deployment. The value range for the *number* argument is 1 to 5.

phone: Displays the result of the most recent batch file deployment for ports connected to IP phones.

Usage guidelines

If you do not specify any parameters, this command displays the result of the most recent batch file deployment performed by using the **smartmc batch-file deploy** command.

Examples

Display the result of the most recent batch file deployment. In this example, the batch file contains the **display smartmc configuration** command.

```
<Sysname> display smartmc batch-file status last 1
```

```
TC ID 1
```

```
Device MAC : 8a73-60c3-0200
```

```
Start Time : 2018-12-24 14:55:39
```

```
End Time : 2018-12-24 14:55:43
```

```
Result :
```

```
<Sysname> display smartmc configuration
```

```
Device role : TC
```

```
TM IP : 192.168.22.103
```

```
TM MAC : 8a73-4faa-0100
```

```
TM sysname : Sysname
```

```
<Sysname>
```

```
TC ID 2
```

```
Device MAC : 8a73-6b31-0300
```

```
Start Time : 2018-12-24 14:55:43
```

```
End Time : 2018-12-24 14:55:48
```

```
Result :
```

```
<Sysname> display smartmc configuration
```

```
Device role : TC
```

```
TM IP : 192.168.22.103
```

TM MAC : 8a73-4faa-0100
TM sysname : Sysname
<Sysname>

Table 2 Command output

Field	Description
TC ID	ID of the member.
Device MAC	MAC address of the member.
Start Time	Batch file deployment start time.
End Time	Batch file deployment end time.
Result	Batch file deployment result in details.

Related commands

```
create batch-file  
smartmc batch-file apply  
smartmc batch-file deploy
```

display smartmc configuration

Use **display smartmc configuration** to display the SmartMC configuration.

Syntax

```
display smartmc configuration
```

Views

Any view

Predefined user roles

network-admin

Examples

Display the SmartMC configuration on the commander.

```
<Sysname> display smartmc configuration
```

```
Device role : TM
```

```
File server:
```

```
Type: FTP
```

```
IP address: 192.168.22.103
```

```
Username: admin
```

```
Port: 21
```

```
VPN instance: N/A
```

```
Directory: /FTP
```

```
Topology-refresh interval : 60(s)
```

```
Backup startup-configuration interval : N/A
```

```
Sync backup number : 5
```

```
Device status : Lack
```

Some configurations are absent on the TM, such as Telnet or LLDP configuration.

Display the commander information on a member.

```
<Sysname> display smartmc configuration
Device role       : TC
TM IP             : 192.168.22.103
TM MAC           : 8288-468d-0100
TM sysname       : Sysname
```

Table 3 Command output

Field	Description
Device role	Role of the device.
File server	File server configuration.
Type	File server type. If no file server is specified, this field displays N/A .
IP address	File server IP address. If no file server is specified, this field displays N/A .
Username	File server username. If no file server is specified, this field displays N/A .
Port	File server port. If no file server is specified, this field displays N/A .
VPN instance	VPN instance to which the file server belongs. If no file server is specified, this field displays N/A .
Directory	Storage directory of files on the file server. If no file server is specified, this field displays N/A .
Topology-refresh interval	Topology refresh interval, in seconds.
Backup startup-configuration interval	Automatic configuration file backup interval, in hours. If no interval is set, this field displays N/A .
Sync backup number	Number of members that can perform configuration backup at the same time.
Device status	Commander status: <ul style="list-style-type: none"> • Normal. • Lack—Lack of configuration, such as NETCONF, Telnet, local user, and LLDP.
TM IP	IP address of the commander. If the member failed to obtain the commander IP address, this field displays N/A .
TM MAC	MAC address of the commander. If the member failed to obtain the commander MAC address, this field displays N/A .
TM sysname	Name of the commander. If the member failed to obtain the commander name, this field displays N/A .
Some configurations are absent on the TM, such as XXX.	This field is available only when the Device status field displays Lack . Lack of configuration will affect SmartMC functions. Please follow the prompt to complete the configuration.

Related commands

```
smartmc backup configuration interval
smartmc backup configuration max-number
smartmc enable
smartmc { ftp-server | sftp-server }
smartmc topology-refresh interval
```


display smartmc device-link

Use **display smartmc device-link** to display connections between devices in the SmartMC network.

Syntax

```
display smartmc device-link
```

Views

Any view

Predefined user roles

network-admin

Examples

Display connections between devices in the SmartMC network.

```
<Sysname> display smartmc device-link
```

```
(TM IP)[192.168.56.20]
```

ID	Hop	LocalPort	LocalIP	PeerPort	PeerIP
0	0	GigabitEthernet1/0/2	192.168.56.20	GigabitEthernet1/0/1	192.168.56.30
1	1	GigabitEthernet1/0/1	192.168.56.30	GigabitEthernet1/0/2	192.168.56.20
1	2	GigabitEthernet1/0/2	192.168.56.30	GigabitEthernet1/0/1	192.168.56.40
2	3	GigabitEthernet1/0/1	192.168.56.40	GigabitEthernet1/0/2	192.168.56.30

Table 4 Command output

Field	Description
TM IP	IP address of the commander.
ID	ID of the commander or member.
Hop	Number of hops between the commander and member.
LocalPort	Local port.
LocalIP	IP address of the local device.
PeerPort	Peer port.
PeerIP	IP address of the peer port.

Related commands

```
smartmc topology-refresh
```

```
smartmc topology-refresh interval
```

display smartmc group

Use **display smartmc group** to display SmartMC group information.

Syntax

```
display smartmc group [ group-name ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

group-name: Specifies a SmartMC group by its name, a case-sensitive string of 1 to 31 characters. If you do not specify this argument, the command displays information about all SmartMC groups.

verbose: Displays detailed SmartMC group information. If you do not specify this keyword, the command displays brief SmartMC group information.

Examples

Display detailed SmartMC group information.

```
<Sysname> display smartmc group verbose
```

```
Group name           : test
```

```
TC count             : 3
```

```
Boot-loader file     :
```

```
Startup-configuration file :
```

```
Rule:
```

```
Match Device-type S5130S-HI
```

TCID	DeviceType	Sysname	IpAddress	MacAddress	Status	Version
1	S5130S-HI	S1	192.168.56.103	0e74-e2fb-0400	Normal	COMWAREV700R001
2	S5130S-HI	S2	192.168.56.102	0e74-ea13-0500	Normal	COMWAREV700R001
3	S5130S-HI	S3	192.168.56.104	0e74-db54-0300	Normal	COMWAREV700R001

Table 5 Command output

Field	Description
GroupName	Name of the SmartMC group.
TC count	Number of members in the SmartMC group.
Boot-loader file	Names of the upgrade startup software files for upgrading the SmartMC group. If no upgrade startup software files are specified, this field displays null.
Startup-configuration file	Name of the configuration file for upgrading the SmartMC group. If no configuration file is specified, this field displays null.
Rule	Match criteria of the SmartMC group.
Match	Match type and its value. The match types include the following: <ul style="list-style-type: none">• Device-type—Matches members by device type.• IP-address—Matches members by IP address.• MAC-address—Matches members by MAC address.
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Version	Software version of the member.
Status	Operating status of the member: <ul style="list-style-type: none">• Offline—The member is offline.• Normal—The member is online.

Related commands

match

`smartmc group`

display smartmc replace status

Use `display smartmc replace status` to display faulty member replacement status.

Syntax

`display smartmc replace status`

Views

Any view

Predefined user roles

network-admin

Examples

```
# Display faulty member replacement status.
<Sysname> display smartmc replace status
Faulty ID      : 2
Faulty MAC     : 94e2-cdcb-0600
Replacement ID : 3
Replacement MAC: 2443-5f8c-0200
Mode           : Manual
Status         : Successful
Start time     : 2017-03-21 15:01:31
End time       : 2017-03-21 15:01:40
```

Table 6 Command output

Field	Description
Faulty ID	ID of the faulty member.
Faulty MAC	MAC address of the faulty member.
Replacement ID	ID of the new member.
Replacement MAC	MAC address of the new member.
Mode	Replacement method, which can be Manual or Auto .
Status	Replacement status: <ul style="list-style-type: none">• Successful.• Failed.• Replacing.• Timeout.
Start time	Replacement start time
End time	Replacement end time.

Related commands

`smartmc auto-replace enable`

`smartmc replace`

display smartmc resource-monitor

Use `display smartmc resource-monitor` to display resource monitoring information.

Syntax

```
display smartmc resource-monitor [ cpu | memory | temperature ] * [ tc  
tc-id | tm ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

cpu: Displays CPU usage.

memory: Displays memory usage.

temperature: Displays temperature information.

tc tc-id: Specify a member by its ID in the range of 1 to 255.

tm: Specify the commander.

Usage guidelines

This command displays CPU usage, memory usage, and temperature information of the commander and members on the commander. For packet dropping information, log in to the Web interface of the commander and access the **SmartMC > Intelligent O&M > Resource monitoring** page.

If you do not specify a resource type, this command displays the resource monitoring information of all types.

If you do not specify a member or the commander, this command displays the resource monitoring information for the commander and all members.

Examples

Display the resource monitoring information for member 1.

```
<Sysname> display smartmc resource-monitor tc 1
```

```
TC 1
```

```
Collection time : 2017-07-25 18:02:30
```

```
Slot 1:
```

```
CPU 0 CPU usage: 1%
```

```
Memory usage   : 587076/903332
```

```
Temperature    : 30
```

Table 7 Command output

Field	Description
Collection time	Time when the resource monitoring information was collected.

Related commands

```
smartmc resource-monitor
```

display smartmc resource-monitor configuration

Use **display smartmc resource-monitor configuration** to display resource monitoring configuration.

Syntax

```
display smartmc resource-monitor configuration
```

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command displays CPU usage, memory usage, and temperature monitoring configuration of the commander. You can view the status of packet dropping monitoring by using the **display current-configuration | include smartmc** command.

Examples

Display resource monitoring configuration.

```
<Sysname> display smartmc resource-monitor configuration
```

ID	MacAddress	CPU	Memory	Temperature
1	1234-2222-3333	Y	N	N
2	1234-2222-3334	Y	N	N
3	1234-2222-3335	Y	N	N

Table 8 Command output

Field	Description
ID	Device ID.
MacAddress	MAC address of the device.
CPU	CPU usage monitoring status: <ul style="list-style-type: none">• Y—CPU usage monitoring is enabled.• N—CPU usage monitoring is disabled.• —The device does not support CPU usage monitoring.
Memory	Memory usage monitoring status: <ul style="list-style-type: none">• Y—Memory usage monitoring is enabled.• N—Memory usage monitoring is disabled.• —The device does not support memory usage monitoring.
Temperature	Temperature monitoring status: <ul style="list-style-type: none">• Y—Temperature monitoring is enabled.• N—Temperature monitoring is disabled.• —The device does not support temperature monitoring.

Related commands

smartmc resource-monitor

display smartmc tc

Use **display smartmc tc** to display member information.

Syntax

```
display smartmc tc [ tc-id ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255. If you do not specify a member, this command displays information about all members.

verbose: Displays detailed member information. If you do not specify this keyword, the command displays brief member information.

Examples

Display brief information about all members.

```
<Sysname> display smartmc tc
```

TCID	DeviceType	Sysname	IpAddress	MacAddress	Status	Version
1	S5130S-HI	S1	192.168.22.104	201c-e7c3-0300	Normal	COMWAREV700R001

Table 9 Command output

Field	Description
TCID	ID of the member.
DeviceType	Device type of the member.
Sysname	Device name of the member.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Status	Operating status of the member: <ul style="list-style-type: none">• Normal—The member is operating correctly.• Offline—The member is offline.
Version	Software version of the member.

Display detailed information about all members.

```
<Sysname> display smartmc tc verbose
```

```
TC ID                : 1
Adding method        : Manual
Sysname              : S1
Model                : S5130S-52S-HI
Device type          : S5130S-HI
SYSOID               : 1.3.6.1.4.1.25506
MAC address          : 0e74-e2fb-0400
IP address            : 192.168.56.103
Boot image           :
Boot image version    :
System image          :
System image version  :
Current-configuration file :
Uptime                : 2 days, 3 hours, 4 minutes
System CPU usage      : 0%
System memory usage   : 0%
Status                : Offline
Boot-loader file      :
Startup-configuration file :
```

Table 10 Command output

Field	Description
TC ID	ID of the member.
Adding method	Method through which the member is added to the SmartMC network: <ul style="list-style-type: none"> Manual. Auto.
Sysname	Device name of the member.
Model	Device model of the member.
Device type	Device type of the member.
SYSOID	SYSOID of the member.
MAC address	MAC address of the member.
IP address	IP address of the member.
Boot image	Boot image file that the member runs.
Boot image version	Version of the boot image file.
System image	System image file that the member runs.
System image version	Version of the system image file.
Current-configuration file	Current startup configuration file used by the member.
Uptime	Operation duration of the member.
System CPU usage	CPU usage on the member.
System memory usage	Memory usage on the member.
Status	Operating status of the member: <ul style="list-style-type: none"> Normal—The member is operating correctly. Offline—The member is offline.
Boot-loader file	Upgrade startup software files.
Startup-configuration file	Upgrade configuration file.

display smartmc tc log buffer

Use **display smartmc tc log buffer** to display log information in the log buffer on a member.

Syntax

```
display smartmc tc tc-id log buffer [ module module-name [ mnemonic mnemonic-value ] ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255.

module *module-name*: Specifies a module by its name, a case-insensitive string of 1 to 8 characters. To display module names, use the **info-center source** command (see information center commands in *Network Management and Monitoring Command Reference*).

mnemonic *mnemonic-value*: Specifies a mnemonic, a case-insensitive string of 1 to 32 characters.

Examples

Display the log information for the SHELL module with the SHELL_CMD mnemonic for member 1.

```
<Sysname> display smartmc tc 1 log buffer module SHELL mnemonic SHELL_CMD
```

```
Time      : 2017-07-15 13:51:46
```

```
Level     : Informational
```

```
Module    : SHELL
```

```
Mnemonic  : SHELL_CMD
```

```
Content   : -Line=con0-IPAddr=**-User=**; Command is qu
```

```
Time      : 2017-07-15 13:51:39
```

```
Level     : Informational
```

```
Module    : SHELL
```

```
Mnemonic  : SHELL_CMD
```

```
Content   : -Line=con0-IPAddr=**-User=**; Command is local-user admin
```

Table 11 Command output

Field	Description
Time	Time when the log was generated.
Level	Log level.

display smartmc tc log restart

Use **display smartmc tc log restart** to display the restart log information for a member.

Syntax

```
display smartmc tc tc-id log restart
```

Views

Any view

Predefined user roles

network-admin

Parameters

tc-id: Specifies a member by its ID in the range of 1 to 255.

Usage guidelines

In addition to saving the logs generated by modules to the log buffer, a member sends restart logs to the commander. The commander creates a restart log buffer for each member to store their restart logs.

The commander stores a maximum of 10 restart logs for each member. The most recent restart log overwrites the oldest one when there are more than 10 restart logs for a member.

You can also use the **display smartmc tc *tc-id* log buffer module SYSLOG mnemonic SYSLOG_RESTART** command to display the restart log information.

Examples

```
# Display the restart log information for member 1.
<Sysname> display smartmc tc 1 log restart
Time      : 2017-07-15 13:51:46
Level     : Informational
Module    : SYSLOG
Mnemonic  : SYSLOG_RESTART
Content   : System restarted -- HPE Comware Software.
```

Table 12 Command output

Field	Description
Time	Time when the log was generated.
Level	Log level.

Related commands

```
display smartmc tc log buffer
```

display smartmc upgrade status

Use `display smartmc upgrade status` to display member upgrade status.

Syntax

```
display smartmc upgrade status
```

Views

Any view

Predefined user roles

network-admin

Examples

```
# Display member upgrade status.
<Sysname> display smartmc upgrade status
ID      IpAddress      MacAddress      Status      UpdateTime      UpdateFile
1       192.168.56.1      82dd-a434-0200  Finished    Immediately      bootloader.ipe
2       192.168.56.103   5caf-2e5f-0100  Finished    Immediately      bootloader.ipe
```

Table 13 Command output

Field	Description
ID	ID of the member.
MacAddress	MAC address of the member.
IpAddress	IP address of the member.
Status	Upgrade status: <ul style="list-style-type: none">• Waiting—The member is waiting for downloading the upgrade file.• Download-failed—The member failed to download the upgrade file.• Download-finished—The member has downloaded the upgrade file.• Downloading—The member is downloading the upgrade file.• Updating—The member is upgrading.• Finished—The member has finished upgrading.

Field	Description
	<ul style="list-style-type: none"> Failed—The member failed to upgrade. Unknown—The upgrade status of the member is unknown.
Updated File	Name of the upgrade file.
UpdateTime	Upgrade time: <ul style="list-style-type: none"> Immediately—Upgrade at once. Delay(m)—Upgrade after the specified delay. Time(HH:MM)—Upgrade at the specified time.

Related commands

`smartmc upgrade group`

`smartmc upgrade tc`

display smartmc vlan

Use `display smartmc vlan` to display VLAN creation results for members.

Syntax

`display smartmc vlan`

Views

Any view

Predefined user roles

network-admin

Examples

Display VLAN creation results.

<Sysname> `display smartmc vlan`

ID	IpAddress	MacAddress	Vlan	Status
1	192.168.22.222	703d-15ad-cd02	2	Success
2	192.168.22.3	24ff-2264-0100	2	Success
3	192.168.22.4	24ff-2f74-0200	2	Success
4	192.168.22.223	487a-dac8-29ba	2	Success

Table 14 Command output

Field	Description
ID	Member ID.
IpAddress	IP address of the member.
MacAddress	MAC address of the member.
Vlan	VLAN created for the member.
Status	VLAN creation status: <ul style="list-style-type: none"> Processing—The VLAN is being created. Success—The VLAN has been created successfully. Failure. The port xxx is not an access port—The VLAN fails to be created, because ports connected to non-SmartMC devices are not access ports. Failure. xxx not exist—The VLAN fails to be created, because all access ports are connected to SmartMC devices.

Related commands

smartmc vlan

match

Use **match** to set a match criterion to add all matching members to a SmartMC group.

Use **undo match** to delete a match criterion.

Syntax

```
match { device-type device-type | ip-address ip-address { ip-mask-length  
| ip-mask } | mac-address mac-address mac-mask-length }
```

```
undo match { device-type device-type | ip-address ip-address  
{ ip-mask-length | ip-mask } | mac-address mac-address mac-mask-length }
```

Default

No match criterion is set.

Views

SmartMC group view

Predefined user roles

network-admin

Parameters

device-type *device-type*: Sets a device type match criterion.

ip-address *ip-address* { *ip-mask-length* | *ip-mask* }: Sets an IP address match criterion. The *ip-address* argument specifies an IP address in dotted decimal notation. The *ip-mask* argument specifies the subnet mask in dotted decimal notation. The *ip-mask-length* argument specifies the subnet mask length in the range of 1 to 32.

mac-address *mac-address* *mac-mask-length*: Sets a MAC address match criterion. The *mac-address* argument specifies a MAC address in the format of *H-H-H*. The *mac-mask-length* argument specifies the mask length in the range of 1 to 48.

Examples

Create a SmartMC group named **a** and add members in subnet 192.168.1.0/24 to the group.

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

```
[Sysname] smartmc group a
```

```
[Sysname-smartmc-group-a] match ip-address 192.168.1.0 24
```

Related commands

smartmc group

display smartmc group

smartmc auto-link-aggregation enable

Use **smartmc auto-link-aggregation enable** to enable automatic Ethernet link aggregation.

Use **undo smartmc auto-link-aggregation enable** to disable automatic Ethernet link aggregation.

Syntax

```
smartmc auto-link-aggregation enable
```

```
undo smartmc auto-link-aggregation enable
```

Default

Automatic Ethernet link aggregation is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Automatic Ethernet link aggregation is performed only between member devices.

Enabling or disabling automatic Ethernet link aggregation might cause network flapping, and the members might go offline for a short period of time.

Examples

```
# Enable automatic Ethernet link aggregation.
<Sysname> system-view
[Sysname] smartmc auto-link-aggregation enable
```

smartmc auto-replace enable

Use **smartmc auto-replace enable** to enable the automatic faulty member replacement feature.

Use **undo smartmc auto-replace enable** to disable the automatic faulty member replacement feature.

Syntax

```
smartmc auto-replace enable
undo smartmc auto-replace enable
```

Default

The automatic faulty member replacement feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To perform an automatic fault replacement, first enable this feature on the commander, and then perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Examples

```
# Enable the automatic faulty member replacement feature.
<Sysname> system-view
[Sysname] smartmc auto-replace enable
```

Related commands

`smartmc replace`

smartmc backup configuration

Use `smartmc backup configuration` to manually back up the configuration file on members.

Syntax

```
smartmc backup configuration { group group-name-list | tc [ tc-id-list ] }
```

Views

System view

Predefined user roles

network-admin

Parameters

group *group-name-list*: Specifies a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a device or a range of devices in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 0 to 255, with 0 representing the commander and 1 to 255 representing members. If you do not specify the commander or any members, all devices will perform configuration backup.

Usage guidelines

After you execute this command, the members immediately save the running configuration to the next-startup configuration files and upload the configuration files to the file server.

The backup configuration files are named in the format of *bridge MAC address_backup.cfg*.

Examples

Back up the configuration file on member 1, member 2, member 3, and member 4.

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

```
[Sysname] smartmc backup configuration tc 1 to 4
```

Back up the configuration file on all members in SmartMC groups **test1**, **test2**, and **test3**.

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

```
[Sysname] smartmc backup configuration group test1 test2 test3
```

Related commands

`display smartmc configuration`

`smartmc backup configuration interval`

smartmc backup configuration max-number

Use `smartmc backup configuration max-number` to set the maximum number of members that can perform automatic configuration backup at the same time.

Use `undo smartmc backup configuration max-number` to restore the default.

Syntax

```
smartmc backup configuration max-number max-number
```

```
undo smartmc backup configuration max-number
```

Default

A maximum of five members can perform automatic configuration backup at the same time.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of members that can perform automatic configuration backup at the same time, in the range of 2 to 20.

Usage guidelines

The maximum number of members that can perform automatic configuration at the same time is limited by the performance of the file server. If automatic configuration backup fails, set the maximum number of members to a smaller value.

Examples

```
# Specify that a maximum of 10 members can perform automatic configuration backup at the same time.
<Sysname> system-view
[Sysname] smartmc backup configuration max-number 10
```

Related commands

```
display smartmc configuration
smartmc backup configuration
smartmc backup configuration interval
```

smartmc backup configuration interval

Use **smartmc backup configuration interval** to enable the automatic configuration file backup feature and set the automatic backup interval.

Use **undo smartmc backup configuration interval** to restore the default.

Syntax

```
smartmc backup configuration interval interval
undo smartmc backup configuration interval
```

Default

The automatic configuration file backup feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the automatic configuration file backup interval in the range of 1 to 720 hours.

Usage guidelines

This command enables the commander and members to back up their configuration files by saving the running configuration to the files and then uploading them to the file server. When you execute

this command, the commander and members immediately perform a backup. After that, they back up the configuration files at the specified interval. The backup configuration files are named in the format of *bridge MAC address_backup.cfg*.

Examples

Enable the automatic configuration file backup feature and set the backup interval to 24 hours.

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

```
[Sysname] smartmc backup configuration interval 24
```

Related commands

display smartmc configuration

smartmc backup configuration

smartmc batch-file apply

Use **smartmc batch-file apply** to specify a batch file to deploy to ports connecting APs or IP phones.

Use **undo smartmc batch-file apply** to remove a batch file specified for ports connecting APs or IP phones.

Syntax

```
smartmc batch-file batch-file-name apply { ap | phone }
```

```
undo smartmc batch-file apply { ap | phone }
```

Default

No batch file is specified for ports connecting APs or IP phones.

Views

System view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies a batch file by its name, a case-insensitive string of 1 to 255 characters.

ap: Specifies ports connecting APs.

phone: Specifies ports connecting IP phones.

Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration.

When the commander first detects the association of an AP or IP phone on a port through LLDP, it deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

If the AP or IP phone disconnects from the port, the configurations on the port remain. When a new device comes online from the port, configurations used by the port depend on the new device type.

- If the new device is an AP or IP phone and has the same type as the disconnected device, the configurations on the port remain unchanged.
- If the new device is an AP or IP phone but has a different type as the disconnected device, the commander deploys the command lines in the specified batch file to the port. If no batch file is specified for the device type, the configurations on the port remain unchanged.

- If the new device is neither an AP nor an IP phone, the configurations on the port remain unchanged.

To disable the commander from deploying a batch file to ports, remove the specified batch file or execute the **undo smartmc batch-file-apply enable** command to disable batch file deployment.

Examples

Specify batch file **ap.cmdset** for ports connecting APs or IP phones.

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

```
[Sysname] smartmc batch-file ap.cmdset apply ap
```

Related commands

create batch-file

smartmc batch-file-apply enable

smartmc batch-file deploy

Use **smartmc batch-file deploy** to deploy bulk command lines to a list of members or SmartMC groups.

Syntax

```
smartmc batch-file batch-file-name deploy { group group-name-list | tc tc-id-list }
```

Views

System view

Predefined user roles

network-admin

Parameters

batch-file-name: Specifies the name of a batch file, a case-insensitive string of 1 to 255 characters.

group *group-name-list*: Specifies a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* **to** *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

Examples

Deploy batch file **startup.cmdset** to SmartMC group **testgroup**.

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

```
[Sysname] smartmc batch-file startup.cmdset deploy group testgroup
```

Related commands

create batch-file

display smartmc batch-file status

smartmc batch-file-apply enable

Use **smartmc batch-file-apply enable** to enable batch file deployment.

Use **undo smartmc batch-file-apply enable** to disable batch file deployment.

Syntax

```
smartmc batch-file-apply enable
undo smartmc batch-file-apply enable
```

Default

Batch file deployment is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

With batch file deployment enabled, the commander automatically deploys configurations in the specified batch file to a port connecting an AP or IP phone, simplifying access port configuration. To disable the commander from deploying a batch file to ports, remove the specified batch file or disable batch file deployment.

Examples

```
# Disable batch file deployment.
<Sysname> system-view
[Sysname] undo smartmc batch-file-apply enable
```

Related commands

```
smartmc batch-file apply
```

smartmc enable

Use **smartmc enable** to enable SmartMC and set the device role.

Use **undo smartmc enable** to disable SmartMC.

Syntax

```
smartmc { tc | tm username username password { cipher | simple } string }
enable
undo smartmc enable
```

Default

SmartMC is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

tc: Enables SmartMC and sets the device role to member.

tm: Enables SmartMC and sets the device role to commander.

username *username*: Specifies a username for the local user, a case-sensitive string of 1 to 55 characters.

password: Specifies a password for the local user.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

A SmartMC network must have one and only one commander.

To enable SmartMC, execute this command on both the commander and members. To configure the other SmartMC features, execute associated commands only on the commander.

If you change the role of the commander to member or disable SmartMC on the commander, all SmartMC settings in its running configuration will be cleared.

SmartMC fails to be enabled if ACL resources are insufficient. If ACL resources are insufficient, use the **undo acl** command to delete unnecessary ACLs and then enable SmartMC. You can execute the **display acl** command to view ACL configuration and match statistics. For more information about ACLs, see *ACL and QoS Configuration Guide*.

SmartMC fails to be enabled if ports 80 and 443 have been used.

If you execute this command multiple times, the most recent configuration takes effect. You can execute the command to change the device role or the password.

Examples

Enable SmartMC and set the device role to member.

```
<Sysname> system-view  
[Sysname] smartmc tc enable
```

smartmc { ftp-server | sftp-server }

Use **smartmc { ftp-server | sftp-server }** to configure the file server information.

Use **undo smartmc { ftp-server | sftp-server }** to delete the file server information.

Syntax

```
smartmc { ftp-server | sftp-server } { ipv4-address | ipv6 ipv6-address }  
[ port port ] [ vpn-instance vpn-instance-name ] [ directory directory ]  
username username password { cipher | simple } string  
undo smartmc { ftp-server | sftp-server }
```

Default

No file server information is configured.

Views

System view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies an FTP server.

sftp-server: Specifies an SFTP server.

ipv4-address: Specifies the IPv4 address of the file server.

ipv6 ipv6-address: Specifies the IPv6 address of the file server.

port *port*: Specifies the port number of the file server, in the range of 1 to 65535. The default port for an FTP server and an SFTP server is 21 and 22, respectively.

vpn-instance *vpn-instance-name*: Specifies the name of the MPLS L3VPN instance to which the file server belongs, a case-sensitive string of 1 to 31 characters. If you do not specify this option, the command considers that the file server is in the public network.

directory *directory*: Specifies the working directory of the file server, a case-insensitive string. By default, the root directory is used.

username *username*: Specifies the file server username, a case-sensitive string of 1 to 55 characters.

password: Specifies the file server password.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

You can specify only one file server. If you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the file server type to FTP, and specify the server IP address, username, and password as 192.168.22.19, **admin**, and **hello12345**, respectively.

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

```
[Sysname] smartmc ftp-server 192.168.22.19 username admin password simple hello12345
```

Related commands

display smartmc configuration

smartmc group

Use **smartmc group** to create a SmartMC group and enter its view, or enter the view of an existing SmartMC group.

Use **undo smartmc group** to delete a SmartMC group.

Syntax

smartmc group *group-name*

undo smartmc group *group-name*

Default

No SmartMC groups exist.

Views

System view

Predefined user roles

network-admin

Parameters

group-name: Specifies the name of the SmartMC group, a case-sensitive string of 1 to 31 characters.

Usage guidelines

When you perform the following operations, you can specify a SmartMC group to apply the operations to all members in the group:

- Startup software upgrade.
- Configuration file upgrade.
- Configuration deployment.

Examples

```
# Create SmartMC group testgroup.  
<Sysname> system-view  
[Sysname] smartmc group testgroup  
[Sysname-smartmc-group-testgroup]
```

Related commands

match

smartmc outbound

Use **smartmc outbound** to configure an outgoing interface for the SmartMC network.

Use **undo smartmc outbound** to restore the default.

Syntax

```
smartmc outbound  
undo smartmc outbound
```

Default

No interface is used as an outgoing interface, and the SmartMC network cannot communicate with outside networks.

Views

VLAN interface view

Predefined user roles

network-admin

Usage guidelines

VLAN interface 1 cannot be used as an outgoing interface, because the SmartMC network is established in VLAN 1.

Examples

```
# Configure GigabitEthernet 1/0/1 as an outgoing interface for the SmartMC network.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] smartmc outbound
```

smartmc resource-monitor

Use **smartmc resource-monitor** to enable resource monitoring.

Use **undo smartmc resource-monitor** to disable resource monitoring.

Syntax

```
smartmc resource-monitor [ cpu | memory | packet-drop | temperature ] *  
[ group group-name-list | tc { tc-id-list | mac-address mac-address } | tm ]  
  
undo smartmc resource-monitor [ cpu | memory | packet-drop | temperature ]  
* [ group group-name-list | tc { tc-id-list | mac-address mac-address } | tm ]
```

Default

Resource monitoring is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

cpu: Enables CPU usage monitoring.

memory: Enables memory usage monitoring.

packet-drop: Enables packet dropping monitoring.

temperature: Enables temperature monitoring.

group group-name-list: Specifies the SmartMC groups to monitor. You can specify a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc: Specifies the members to monitor.

tc-id-list: Specifies a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

mac-address mac-address: Specifies a member by its MAC address in the format of H-H-H.

tm: Enables resource monitoring on the commander.

Usage guidelines

Packet dropping monitoring monitors packet dropping on members and on interfaces.

If you do not specify a resource type, this command enables resource monitoring for all resource types.

If you do not specify a device to monitor (member or the commander), this command enables resource monitoring on the commander and all members.

Examples

```
# Enable resource monitoring for all resource types on member 1 through member 3.
```

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

```
[Sysname] smartmc resource-monitor tc 1 to 3
```

Related commands

```
display smartmc resource-monitor
```

```
smartmc resource-monitor interval
```

```
smartmc resource-monitor max-age
```

smartmc resource-monitor interval

Use **smartmc resource-monitor interval** to set the interval for the commander to obtain resource monitoring information.

Use **undo smartmc resource-monitor interval** to restore the default.

Syntax

```
smartmc resource-monitor interval interval
```

```
undo smartmc resource-monitor interval
```

Default

The interval for the commander to obtain resource monitoring information is 1 minute.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for the commander to obtain resource monitoring information, in the range of 1 to 60 minutes.

Usage guidelines

For packet dropping monitoring, the specified interval applies only to obtaining of member packet dropping information. Because of the great amount of interface information, the commander obtains interface packet dropping information from members only when Web displaying is requested.

Examples

Set the interval for the commander to obtain resource monitoring information to 5 minutes.

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

```
[Sysname] smartmc resource-monitor interval 5
```

Related commands

```
display smartmc resource-monitor
```

```
smartmc resource-monitor
```

smartmc resource-monitor max-age

Use **smartmc resource-monitor max-age** to set the aging time for resource monitoring information.

Use **undo smartmc resource-monitor max-age** to restore the default.

Syntax

```
smartmc resource-monitor max-age max-age
```

```
undo smartmc resource-monitor max-age
```

Default

The aging time for resource monitoring information is 24 hours.

Views

System view

Predefined user roles

network-admin

Parameters

max-age: Specifies the aging time for resource monitoring information, in the range of 1 to 168 hours.

Usage guidelines

For packet dropping monitoring, the specified aging time applies only to member packet dropping information. Each member saves its interface packet dropping information for as long as 30 days.

To view interface packet dropping information, log in to the Web interface of the commander and access the **SmartMC > Intelligent O&M > Resource monitoring** page. You can view information in the past 1 hour, 1 day, or 30 days.

Examples

```
# Set the aging time for resource monitoring information to 1 hour.
```

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

```
[Sysname] smartmc resource-monitor max-age 1
```

Related commands

```
display smartmc resource-monitor
```

```
smartmc resource-monitor
```

smartmc replace

Use **smartmc replace** to manually replace a faulty member.

Syntax

```
smartmc replace tc tc-id1 faulty-tc tc-id2
```

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id1*: Specifies the ID of the new member, in the range of 1 to 255.

faulty-tc *tc-id2*: Specifies the ID of the faulty member, in the range of 1 to 255.

Usage guidelines

Before you execute this command, perform the following tasks:

1. Install the new member at the location where the faulty member was installed.
2. Connect all cables to the new member.

Make sure the new member and the faulty member have the same neighbor relationship, device model, and IRF member ID.

Examples

```
# Replace faulty member 5 with new member 10.
```

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

```
[Sysname] smartmc replace tc 10 faulty-tc 5
```

Related commands

```
display smartmc replace status
smartmc auto-replace enable
```

smartmc tc boot-loader

Use **smartmc tc boot-loader** to specify the upgrade startup software files for a member.

Use **undo smartmc tc boot-loader** to remove the configuration.

Syntax

```
smartmc tc tc-id boot-loader { ipe-filename | boot boot-filename system
system-filename }
undo smartmc tc tc-id boot-loader
```

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id*: Specifies a member by its ID in the range of 1 to 255.

ipe-filename: Specifies an IPE software file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.ipe** extension.

boot *boot-filename*: Specifies a boot image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

system *system-filename*: Specifies a system image file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.bin** extension.

Examples

Specify upgrade boot image **boot.bin** and upgrade system image **system.bin** for member 1.

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

```
[Sysname] smartmc tc 1 boot-loader boot boot.bin system system.bin
```

Related commands

```
display smartmc tc
```

smartmc tc device-type

Use **smartmc tc device-type** to define a member type on the commander.

Use **undo smartmc tc device-type** to delete a member type.

Syntax

```
smartmc tc sysoid sysoid device-type device-type
undo smartmc tc sysoid sysoid device-type device-type
```

Views

System view

Predefined user roles

network-admin

Parameters

sysoid *sysoid*: Specifies the SYSOID of a member.

device-type *device-type*: Specifies a member type.

Usage guidelines

A device type can correspond to multiple device models. You can identify different device models with different SYSOIDs by specifying a SYSOID for each device model. The commander identifies member types by SYSOID.

The system predefines the device types for some device models based on SYSOIDs. For device models without predefined device types, you must define their member types by SYSOID manually. If you do not do so, the commander cannot identify the types of such devices.

You cannot modify the predefined device types.

Before defining a device type for a member, you can use the **display smartmc tc** command to determine whether the member has a predefined one.

- If the member has been predefined with one device type, the **DeviceType** field displays the actual predefined device type.
- If the member does not have a predefined device type, the **DeviceType** field displays **unknown**.

To obtain the SYSOID of a member, use the **display smartmc tc verbose** command.

Examples

Define a member type by specifying the SYSOID as 1.3.6.1.4.1.25506.1.1588 and the member type as SW.

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

```
[Sysname] smartmc tc sysoid 1.3.6.1.4.1.25506.1.1588 device-type SW
```

smartmc tc password

Use **smartmc tc password** to modify the password for the default user (admin) on members.

Use **undo smartmc tc password** to restore the default.

Syntax

```
smartmc tc password [ cipher ] string
```

```
undo smartmc tc password
```

Default

The password for the default user on members is **admin**.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form. If you do not specify this keyword, the command creates a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

During SmartMC network establishment, the commander establishes NETCONF sessions to members and adds them to the network. The default username and password on the members for NETCONF session establishment are **admin** and **admin**. To enhance security, you can perform this task to change the password for the default user **admin** of the members after the commander adds the members to the network.

If the default password cannot meet the password complexity requirements on members, you cannot execute the **undo smartmc tc password** command to restore the default.

Do not modify the password for members that are manually added to the SmartMC network. If you modify the password for a manually added member, you will not be able to manage that member from the commander.

Examples

Configure default user admin on members to use plaintext password **hello12345**.

```
<Sysname> system-view
[Sysname] smartmc tc password hello12345
```

smartmc tc startup-configuration

Use **smartmc tc startup-configuration** to specify the upgrade configuration file for a member.

Use **undo smartmc tc startup-configuration** to remove the configuration.

Syntax

```
smartmc tc tc-id startup-configuration cfg-filename
undo smartmc tc tc-id startup-configuration
```

Views

System view

Predefined user roles

network-admin

Parameters

tc *tc-id*: Specifies a member by its ID in the range of 1 to 255.

cfg-filename: Specifies a configuration file by its name, a case-insensitive string of 5 to 45 characters. The file name must include the **.cfg** extension.

Examples

Specify upgrade configuration file **startup.cfg** for member 1.

```
<Sysname> system-view
[Sysname] smartmc tc 1 startup-configuration startup.cfg
```

Related commands

```
display smartmc tc
```

smartmc topology-refresh

Use **smartmc topology-refresh** to manually refresh the network topology.

Syntax

```
smartmc topology-refresh
```

Views

Any view

Predefined user roles

network-admin

Usage guidelines

To display topology changes, use this command to manually refresh the topology.

Examples

```
# Manually refresh the network topology.  
<Sysname> smartmc topology-refresh
```

Related commands

display smartmc device-link

smartmc topology-refresh interval

Use **smartmc topology-refresh interval** to set the automatic network topology refresh interval.

Use **undo smartmc topology-refresh interval** to restore the default.

Syntax

```
smartmc topology-refresh interval interval  
undo smartmc topology-refresh interval
```

Default

The automatic network topology refresh interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the automatic network topology refresh interval in the range of 60 to 300 seconds.

Examples

```
# Set the automatic network topology refresh interval to 100 seconds.  
<Sysname> system-view  
[Sysname] smartmc topology-refresh interval 100
```

Related commands

display smartmc device-link

smartmc topology-save

Use **smartmc topology-save** to save the current network topology.

Syntax

```
smartmc topology-save
```

Views

System view

Predefined user roles

network-admin

Usage guidelines

This task allows you to save the current network topology to the **topology.dba** file in the flash memory. After the commander reboots, it uses the **topology.dba** file to restore the network topology.

Examples

```
# Save the current network topology
<Sysname> system-view
[Sysname] smartmc topology-save
```

Related commands

display smartmc device-link

smartmc upgrade boot-loader

Use **smartmc upgrade boot-loader** to upgrade the startup software on a list of members or SmartMC groups.

Use **undo smartmc upgrade** delete the startup software upgrade task.

Syntax

```
smartmc upgrade boot-loader { group | tc } list [ delay minutes | time
time ]

smartmc upgrade boot-loader { group | tc } { list { boot boot-filename
system system-filename | file ipe-filename } }<1-40> [ delay delay-time
| time time ]

undo smartmc upgrade
```

Views

System view

Predefined user roles

network-admin

Parameters

group: Specifies the SmartMC groups to be upgraded.

tc: Specifies the members to be upgraded.

list: Specifies a space-separated list of up to 10 member items or SmartMC group items.

- **SmartMC group**—Each item specifies a SmartMC group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

boot *boot-filename*: Specifies a boot image by its name.

system *system-filename*: Specifies a system image by its name.

file *ipe-filename*: Specifies an IPE file by its name, a case-insensitive string of 5 to 45 characters.

delay *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

time *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

Usage guidelines

⚠ CAUTION:

Upgrading the startup software might interrupt services. Before upgrading the startup software, make sure no services will be interrupted.

To use this command to upgrade the startup software on members without specifying the upgrade files, you must first perform one of the following tasks:

- Execute the **smartmc tc boot-loader** command to specify the upgrade files for members.
- Execute the **boot-loader** command to specify the upgrade files for a SmartMC group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or SmartMC group immediately upgrades the startup software and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

Examples

Upgrade startup software images **boot.bin** and **sys.bin** on all members in SmartMC groups **test1** and **test2**.

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

```
[Sysname] smartmc upgrade boot-loader group test1 test2 boot boot.bin system sys.bin
```

Related commands

boot-loader

startup-configuration

smartmc upgrade startup-configuration

Use **smartmc upgrade startup-configuration** to upgrade the configuration file on a list of members or on all members in SmartMC groups.

Use **undo smartmc upgrade** delete the configuration file upgrade task.

Syntax

```
smartmc upgrade startup-configuration { group | tc } list [ delay minutes  
| time time ]
```

```
smartmc upgrade startup-configuration group { list file  
cfg-filename }&<1-40> [ delay delay-time | time time ]
```

```
smartmc upgrade startup-configuration tc { list cfg-filename }&<1-40>  
[ delay delay-time | time time ]
```

```
undo smartmc upgrade
```

Views

System view

Predefined user roles

network-admin

Parameters

group: Specifies the SmartMC groups to be upgraded.

tc: Specifies the members to be upgraded.

list: Specifies a space-separated list of up to 10 member items or SmartMC group items.

- **SmartMC group**—Each item specifies a SmartMC group name, a case-sensitive string of 1 to 31 characters.
- **Member**—Each item specifies a member ID or a range of member IDs in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

file *cfg-filename*: Specifies a configuration file by its name.

delay *delay-time*: Specifies the upgrade delay time in the range of 1 to 1440 minutes.

time *in-time*: Specifies the upgrade time in the format of *hh:mm*. The value range for the *hh* argument is 0 to 23 hours. The value range for the *mm* argument is 0 to 59 minutes.

Usage guidelines

CAUTION:

After you update the configuration file, the configuration in the new configuration file will become the running configuration. Before upgrading the configuration file, make sure the contents of the new configuration file are correct.

To use this command to upgrade the configuration file on members without specifying the upgrade file, you must first perform one of the following tasks:

- Execute the **smartmc tc startup-configuration** command to specify the upgrade file for members.
- Execute the **startup-configuration** command to specify the upgrade file for a SmartMC group.

A member can perform only one upgrade task at a time.

If you execute this command without specifying the delay time or update time, the members or SmartMC group immediately upgrades the configuration file and the upgrade operation cannot be cancelled. If you specify a delay time or upgrade time to perform a scheduled upgrade, the upgrade operation can be cancelled by using the **undo smartmc upgrade** command before it starts.

Examples

Upgrade configuration file **startup.cfg** on all members in SmartMC groups **test1** and **test2**.

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

```
[Sysname] smartmc upgrade boot-loader group test1 test2 file startup.cfg
```

Related commands

boot-loader

startup-configuration

smartmc vlan

Use **smartmc vlan** to create a VLAN for members.

Syntax

```
smartmc vlan vlan-id { group group-name-list | tc tc-id-list }
```

Views

System view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the VLAN ID in the range of 1 to 4094.

group *group-name-list*: Specifies the SmartMC groups for which the VLAN is created. You can specify a space-separated list of up to 10 SmartMC groups. The group name is a case-sensitive string of 1 to 31 characters.

tc *tc-id-list*: Specifies the members for which the VLAN is created. You can specify a space-separated list of up to 10 member items. Each item specifies a member or a range of members in the form of *tc-id1* to *tc-id2*. The value for *tc-id2* must be greater than or equal to the value for *tc-id1*. The value range for the *tc-id* argument is 1 to 255.

Usage guidelines

Execute this command when the network topology is stable. As a best practice, use the **smartmc topology-refresh** command to refresh the network topology before executing this command.

After you execute this command, all access ports on members except the following access ports are assigned to the VLAN:

- Access ports connecting to the commander.
- Access ports connecting to other members.
- Access ports connecting to offline devices. Remove offline devices before configuring this command.

If the VLAN is successfully created but some access ports of a member cannot be assigned to the VLAN, the VLAN memberships of the member is restored to the state before the VLAN is created.

The failure to assign an access port of a member to the created VLAN does not affect the VLAN assignment for other members.

After command execution, you can use the **display smartmc vlan** command to examine the VLAN creation result.

Examples

Create a VLAN for member 1 and member 2.

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

```
[Sysname] smartmc vlan 2 tc 1 to 2
```

As a best practice, execute the **display smartmc vlan** command to verify that the VLAN has been created successfully.

startup-configuration

Use **startup-configuration** to specify an upgrade configuration file for a SmartMC group .

Use **undo startup-configuration** to restore the default.

Syntax

startup-configuration *cfgfile*

undo startup-configuration

Default

No upgrade configuration file is specified for the SmartMC group.

Views

SmartMC group view

Predefined user roles

network-admin

Parameters

cfgfile: Specifies a configuration file by its name, a string of 5 to 45 characters. The file name must include the **.cfg** extension.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Specify configuration file startup.cfg for SmartMC group testgroup.
<Sysname> system-view
[Sysname] smartmc group testgroup
[Sysname-smartmc-group-testgroup] startup-configuration startup.cfg
```


New feature: Configuring interface alarm functions

Configuring interface alarm functions

About this task

With the interface alarm functions enabled, when the number of error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

Restrictions and guidelines

You can configure the error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

An interface that is shut down because of error packet alarms cannot automatically recover. To bring up the interface, execute the **undo shutdown** command on the interface.

To ensure that error packet statistics are accurate, make sure the value for the **interval interval** option is greater than 7.

Enabling interface alarm functions

1. Enter system view.
system-view
2. Enable alarm functions for the interface monitoring module.
snmp-agent trap enable ifmonitor [crc-error]
By default, all alarm functions are enabled for interfaces.

Configuring CRC error packet parameters

1. Enter system view.
system-view
3. Configure global CRC error packet alarm parameters.
ifmonitor crc-error slot slot-number high-threshold high-value low-threshold low-value interval interval [shutdown]
By default, the upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packets.
4. Enter Ethernet interface view.
interface interface-type interface-number
5. Configure CRC error packet alarm parameters for the interface.
port ifmonitor crc-error high-threshold high-value low-threshold low-value interval interval [shutdown]
By default, an interface uses the global CRC error packet alarm parameters.

Command reference

ifmonitor crc-error

Use **ifmonitor crc-error** to configure global CRC error packet alarm parameters.

Use **undo ifmonitor crc-error** to restore the default.

Syntax

```
ifmonitor crc-error slot slot-number high-threshold high-value  
low-threshold low-value interval interval [shutdown ]  
  
undo ifmonitor crc-error slot slot-number
```

Default

The upper threshold is 1000, the lower threshold is 100, and the statistics collection and comparison interval is 10 seconds for CRC error packet alarms.

Views

System view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.
- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

```
# Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms.
```

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

```
[Sysname] ifmonitor crc-error slot 1 high-threshold 5000 low-threshold 400 interval 6
```

Related commands

```
snmp-agent trap enable ifmonitor
```

port ifmonitor crc-error

Use **port ifmonitor crc-error** to configure CRC error packet alarm parameters for an interface.

Use **undo port ifmonitor crc-error** to restore the default.

Syntax

```
port ifmonitor crc-error high-threshold high-value low-threshold low-value interval interval [ shutdown ]
```

```
undo port ifmonitor crc-error
```

Default

An interface uses the global CRC error packet alarm parameters.

Views

Ethernet interface view

Predefined user roles

network-admin

Parameters

high-threshold *high-value*: Specifies the upper threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

low-threshold *low-value*: Specifies the lower threshold for CRC error packet alarms, in the range of 1 to 4294967295 packets.

interval *interval*: Specifies the statistics collection and comparison interval for CRC error packets, in the range of 1 to 65535 seconds.

shutdown: Shuts down an interface when the number of incoming CRC error packets on the interface exceeds the upper threshold. Then, the interface stops forwarding all packets. To recover the interface, execute the **undo shutdown** command on the interface. If you do not specify this keyword, an upper threshold exceeding alarm is generated and the interface enters the alarm state when the number of incoming CRC error packets exceeds the upper threshold on the interface.

Usage guidelines

With the CRC error packet alarm function enabled, when the number of incoming CRC error packets on an interface in normal state within the specified interval exceeds the upper threshold, the interface generates an upper threshold exceeding alarm and enters the alarm state. When the number of incoming CRC error packets on an interface in the alarm state within the specified interval drops below the lower threshold, the interface generates a recovery alarm and restores to the normal state.

You can configure the CRC error packet alarm parameters in system view and interface view.

- The configuration in system view takes effect on all interfaces of the specified slot. The configuration in interface view takes effect only on the current interface.

- For an interface, the configuration in interface view takes priority, and the configuration in system view is used only when no configuration is made in interface view.

When you execute this command multiple times, the most recent configuration takes effect.

Examples

Set the upper threshold to 5000, lower threshold to 400, and statistics collection and comparison interval to 6 seconds for CRC error packet alarms on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port ifmonitor crc-error high-threshold 5000
low-threshold 400 interval 6
```

Related commands

snmp-agent trap enable ifmonitor

snmp-agent trap enable ifmonitor

Use **snmp-agent trap enable ifmonitor** to enable interface alarm functions.

Use **undo snmp-agent trap enable ifmonitor** to disable interface alarm functions.

Syntax

```
snmp-agent trap enable ifmonitor [ crc-error ]
undo snmp-agent trap enable ifmonitor [ crc-error ]
```

Default

Interface alarm functions are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

crc-error: Enables the CRC error packet alarm function for interfaces.

Examples

Enable the CRC error packet alarm function for interfaces.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ifmonitor crc-error
```

New feature: Configuring Option 60 for DHCP requests

Configuring Option 60 for DHCP requests

About this task

Option 60 acts as a vendor class identifier (VCI). You can configure a DHCP client to send a request with Option 60 for the DHCP server to make class-based IP address assignment. When the DHCP server receives a request with Option 60 from a client, the server identifies the user class of the client. Then, the server assigns the client an IP address from the IP range specified for the user class.

By default, Option 60 contains the vendor name and the product name. To define this option for DHCP requests, perform this task.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type interface-number*
3. Configure Option 60 for DHCP requests.
dhcp client class-id { **ascii** *ascii-string* | **hex** *hex-string* }
By default, Option 60 contains the vendor name and the product name.

Command reference

dhcp client class-id

Use **dhcp client class-id** to configure Option 60.

Use **undo dhcp client class-id** to restore the default.

Syntax

```
dhcp client class-id { ascii ascii-string | hex hex-string }  
undo dhcp client class-id
```

Default

Option 60 contains the vendor name and the product name.

Views

Interface view

Predefined user roles

network-admin

Parameters

ascii *ascii-string*: Specifies a case-sensitive ASCII string of 1 to 63 characters as the content in Option 60.

hex *hex-string*: Specifies a case-sensitive hexadecimal string of 4 to 64 characters as the value in Option 60.

Usage guidelines

Option 60 acts as a vendor class identifier (VCI). You can configure a DHCP client to send a request with Option 60 for the DHCP server to make class-based IP address assignment. When the DHCP server receives a request with Option 60 from a client, the server identifies the user class of the client. Then, the server assigns the client an IP address from the IP range specified for the user class.

By default, Option 60 contains the vendor name and the product name. To customize this option, use this command.

Examples

Configure FFFFFFFF as the content of Option 60 on VLAN-interface 10.

```
<Sysname> system-view  
[Sysname] interface vlan-interface 10  
[Sysname-Vlan-interface10] dhcp client class-id hex FFFFFFFF
```

New feature: Configuring the type of port ID TLVs advertised by LLDP

Configuring the type of port ID TLVs advertised by LLDP

About this task

An HPE device determines whether it has an MED neighbor based on received LLDPDUs. If the LLDPDUs contain LLDP-MED TLVs, the device determines that it has an MED neighbor. By default, the device advertises port ID TLVs that contain interface MAC addresses out of interfaces that have MED neighbors. If no MED neighbor exists on an interface, the device advertises port ID TLVs that contain interface names through the interface.

This task enables an HPE device to advertise only port ID TLVs that contain interface names. The media devices from some vendors can obtain interface information from HPE devices only through LLDP. For the media devices to obtain interface names, you must configure HPE devices to generate port ID TLVs based on interface names.

Restrictions and guidelines

Perform this task only when LLDP neighbors must obtain interface names from LLDPDUs. Do not perform this task in any other scenarios.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

Configuring the type of port ID TLVs advertised by LLDP globally

1. Enter system view.

system-view

1. Configure the type of port ID TLVs advertised by LLDP.

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] global  
tlv-config basic-tlv port-id type-id
```

By default, an interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

Configuring the type of port ID TLVs advertised by LLDP on an interface

1. Enter system view.

system-view

2. Enter interface view.

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

2. Configure the type of port ID TLVs advertised by LLDP.

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-config  
basic-tlv port-id type-id
```

By default, an interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

Command reference

lldp global tlv-config basic-tlv port-id

Use **lldp global tlv-config basic-tlv port-id** to set the type of port ID TLVs advertised by LLDP globally.

Use **undo lldp global tlv-config basic-tlv port-id** to restore the default.

Syntax

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] global tlv-config  
basic-tlv port-id type-id
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] global  
tlv-config basic-tlv port-id
```

Default

An interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

Views

System view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command sets the port ID TLV type for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

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

type-id: Specifies a port ID TLV type. The available value is 5, which represents that port ID TLVs contain interface names.

Usage guidelines

This command enables the device to advertise only port ID TLVs that contain interface names. Execute this command if LLDP neighbors must obtain interface names from LLDPDUs.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

Examples

```
# Enable the device to advertise port ID TLVs that contain interface names.
```

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

```
[Sysname] lldp global tlv-config basic-tlv port-id 5
```

Related commands

```
lldp tlv-config basic-tlv port-id
```

lldp tlv-config basic-tlv port-id

Use **lldp tlv-config basic-tlv port-id** to set the type of port ID TLVs advertised by LLDP on an interface.

Use **undo lldp tlv-config basic-tlv port-id** to restore the default.

Syntax

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-config basic-tlv
port-id type-id

undo lldp [ agent { nearest-customer | nearest-nontpmr } ] tlv-config
basic-tlv port-id
```

Default

An interface advertises port ID TLVs that contain interface MAC addresses if it receives LLDP-MED TLVs and advertises port ID TLVs that contain interface names if no LLDP-MED TLVs are received.

Views

Layer 2 Ethernet interface view
Management Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

agent: Specifies an LLDP agent type. If you do not specify an agent type, the command sets the port ID TLV type for nearest bridge agents.

nearest-customer: Specifies nearest customer bridge agents.

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

type-id: Specifies a port ID TLV type. The available value is 5, which represents that port ID TLVs contain interface names.

Usage guidelines

This command enables an interface to advertise only port ID TLVs that contain interface names. Execute this command if LLDP neighbors must obtain interface names from LLDPDUs.

You can configure the port ID TLV type in system view or interface view. The interface-specific setting takes precedence over the global setting.

Examples

```
# Enable GigabitEthernet 1/0/1 to advertise port ID TLVs that contain interface names.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-config basic-tlv port-id 5
```

Related commands

```
lldp global tlv-config basic-tlv port-id
```

New feature: Enabling displaying LLDP local information about all interfaces

Enabling displaying LLDP local information about all interfaces

About this task

This task enables the **display lldp local-information** command to display LLDP local information about all interfaces.

By default, the **display lldp local-information** command displays information about physically up interfaces. The media devices from some vendors can obtain interface information from HPE devices only through LLDP. For the media devices to obtain all interface information, enable the **display lldp local-information** command to display LLDP local information about all interfaces.

Restrictions and guidelines

Perform this task only when LLDP neighbors must obtain all interface information from the device through LLDP.

Procedure

1. Enter system view.

```
system-view
```

1. Enable displaying LLDP local information about all interfaces.

```
lldp local-information all-interface
```

By default, the **display lldp local-information** command displays information about physically up interfaces.

Command reference

lldp local-information all-interface

Use **lldp local-information all-interface** to enable displaying LLDP local information about all interfaces.

Use **undo lldp local-information all-interface** to disable displaying LLDP local information about interfaces not in physically up state.

Syntax

```
lldp local-information all-interface
```

```
undo lldp local-information all-interface
```

Default

The **display lldp local-information** command displays information about physically up interfaces.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the **display lldp local-information** command to display LLDP local information about all interfaces.

By default, the **display lldp local-information** command displays information about physically up interfaces. The media devices from some vendors can obtain interface information from HPE devices only through LLDP. For the media devices to obtain all interface information, enable the **display lldp local-information** command to display LLDP local information about all interfaces.

Examples

```
# Enable displaying LLDP local information about all interfaces.
```

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

```
[Sysname] lldp local-information all-interface
```

Related commands

```
display lldp local-information
```

New feature: PoE forced power supply

Enabling PoE forced power supply

About this task

Before supplying power to a PD, the device performs a detection of the PD. It supplies power to the PD only after the PD passes the detection. If the PD fails the detection but the power provided by the device meets the PD specifications, you can perform this task to enable forced power supply to the PD.

Restrictions and guidelines

This feature enables the device to supply power to a PD directly without performing a detection of the PD. To avoid damaging the PD, make sure the power provided by the device meets the PD specifications before performing this task.

After enabling PoE forced power supply on a PI, the system reserves the maximum power for the PI even if no PD is attached to the PI or the PI is not enabled with PoE. For the maximum power that a PI can deliver, execute the **display poe pse pse-id interface power** command. For the maximum power that the PSE can allocate, execute the **display poe pse** command.

Procedure

1. Enter system view.
system-view
 2. Enter PI view.
interface *interface-type* *interface-number*
 3. Enable PoE forced power supply.
poe force-power
- By default, PoE forced power supply is disabled.

Command reference

poe force-power

Use **poe force-power** to enable PoE forced power supply.

Use **undo poe force-power** to disable PoE forced power supply.

Syntax

```
poe force-power  
undo poe force-power
```

Default

PoE forced power supply is disabled.

Views

PI view

Predefined user roles

network-admin

Usage guidelines

CAUTION:

This command enables the device to supply power to a PD directly without performing a detection of the PD. To avoid damaging the PD, make sure the power provided by the device meets the PD specifications before executing this command.

Before supplying power to a PD, the device performs a detection of the PD. It supplies power to the PD only after the PD passes the detection. If the PD fails the detection but the power provided by the device meets the PD specifications, you can execute this command to enable forced power supply to the PD.

After enabling PoE forced power supply on a PI, the system reserves the maximum power for the PI even if no PD is attached to the PI or the PI is not enabled with PoE. For the maximum power that a PI can deliver, execute the **display poe pse pse-id interface power** command. For the maximum power that the PSE can allocate, execute the **display poe pse** command.

Examples

Enable PoE forced power supply.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe force-power
```

The PD might be damaged if the power provided by the device does not meet the PD power specifications. Continue? [Y/N]:y

Command changes

Modified command: display poe pse

Syntax

```
display poe pse
```

Views

Any view

Change description

Before modification: The output from the **display poe pse** command does not contain the **Max Allocable Power** field.

After modification: The **Max Allocable Power** field was added to the output from the **display poe pse** command. The value for the field is equal to the maximum power of the PSE minus the sum of the maximum powers of all PIs on which PoE forced power supply is enabled.

New feature: Interval at which the SNMP module examines the system configuration for changes

Setting the interval at which the SNMP module examines the system configuration for changes

About this task

This task enables the SNMP module to examine the system configuration for changes at the specified interval and generate a trap and a log if any change is found.

Procedure

1. Enter system view.
system-view
2. Set the interval at which the SNMP module examines the system configuration for changes.
snmp-agent configuration-examine interval *interval*
By default, the SNMP module examines the system configuration for changes at intervals of 600 seconds.

Command reference

snmp-agent configuration-examine interval

Use **snmp-agent configuration-examine interval** to set the interval at which the SNMP module examines the system configuration for changes.

Use **undo snmp-agent configuration-examine interval** to restore the default.

Syntax

```
snmp-agent configuration-examine interval interval  
undo snmp-agent configuration-examine interval
```

Default

By default, the SNMP module examines the system configuration for changes at intervals of 600 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which the SNMP module examines the system configuration for changes. The value is in the range of 1 to 86400, in seconds.

Usage guidelines

This command enables the SNMP module to examine the system configuration for changes at the specified interval and generate a trap and a log if any change is found.

Examples

```
# Set the interval at which the SNMP module examines the system configuration for changes to 600 seconds.
<sysname> system-view
[sysname] snmp-agent configuration-examine interval 600
```

New feature: Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users

Enabling generation of dynamic IPSG binding entries for 802.1X authenticated users

About this task

❗ IMPORTANT:

This feature must operate in conjunction with the IP source guard (IPSG) feature.

By default, the device generates a dynamic IPv4SG or IPv6SG binding entry for an 802.1X authenticated user after the user obtains a static or DHCP assigned IP address.

To allow only 802.1X users with DHCP assigned IP addresses to access the network, perform the following operations:

- Enable IPSG.
- Disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.
- Enable DHCP snooping. The device will generate IPv4SG or IPv6SG binding entries for the users based on DHCP snooping.

For more information about IPSG, see IP source guard in *Security Configuration Guide*.

Restrictions and guidelines

This feature takes effect only on 802.1X users that come online after the feature is enabled. If the IP address of an online 802.1X user changes, the device will update the dynamic IPv4SG or IPv6SG binding entry for the user.

Disabling this feature does not delete the existing dynamic IPv4SG or IPv6SG binding entries for online 802.1X users. If the IP address of an online 802.1X user changes after the feature is disabled, the device will delete the dynamic IPv4SG or IPv6SG binding entry for the user.

Procedure

1. Enter system view.
system-view
2. Enter interface view.
interface *interface-type* *interface-number*
3. Enable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.
dot1x { ip-verify-source | ipv6-verify-source } enable

By default, generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users is enabled.

dot1x { ip-verify-source | ipv6-verify-source } enable

Use **dot1x { ip-verify-source | ipv6-verify-source } enable** to enable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

Use **undo dot1x { ip-verify-source | ipv6-verify-source } enable** to disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users.

Syntax

```
dot1x { ip-verify-source | ipv6-verify-source } enable
undo dot1x { ip-verify-source | ipv6-verify-source } enable
```

Default

Generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users is enabled.

Views

Layer 2 Ethernet interface view
Layer 2 aggregate interface view

Predefined user roles

network-admin
mdc-admin

Usage guidelines

❗ IMPORTANT:

This feature must operate in conjunction with the IP source guard (IPSG) feature.

The **dot1x { ip-verify-source | ipv6-verify-source } enable** command takes effect only on 802.1X users that come online after the command is used. If the IP address of an online 802.1X user changes, the device will update the dynamic IPv4SG or IPv6SG binding entry for the user.

The **undo dot1x { ip-verify-source | ipv6-verify-source } enable** command does not delete the existing dynamic IPv4SG or IPv6SG binding entries for online 802.1X users. If the IP address of an online 802.1X user changes after the command is used, the device will delete the dynamic IPv4SG or IPv6SG binding entry for the user.

Examples

Disable generation of dynamic IPv4SG or IPv6SG binding entries for 802.1X authenticated users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x ip-verify-source enable
```

New feature: Automated IPv6 underlay network deployment for VCF fabric

About automated IPv6 underlay network deployment

As from this software version, the VCF fabric feature supports automated IPv6 underlay network deployment. The deployment procedure is the same as that of automated IPv4 underlay network deployment.

In an IPv6 VCF fabric, the controller collects the topology automatically. You do not need to specify a master spine node.

Command reference

None.

Modified feature: Setting the port status detection timer

Feature change description

As from this release, the value range for the port status detection timer is changed to 0 to 3600 seconds.

The device starts a port status detection timer when a port is shut down by a protocol such as LLDP and loop detection. Once the timer expires, the device brings up the port so the port status reflects the port's physical status. For example, loop detection shuts down a looped interface to disable the interface from receiving or sending frames. The device automatically sets the interface to the forwarding state after the port status detection timer expires.

Command changes

Modified command: shutdown-interval

Syntax

```
shutdown-interval interval  
undo shutdown-interval
```

Views

System view

Change description

Before modification: The value range for the *interval* argument is 0 to 300.

After modification: The value range for the *interval* argument is 0 to 3600.

Modified feature: 802.1X EAD assistant

Feature change description

As from this version, you can use the **dot1x ead-assistant permit authentication-escape** command to enable support for 802.1X Auth-Fail and critical VLANs in 802.1X EAD assistant.

Command changes

New command: dot1x ead-assistant permit authentication-escape

Use **dot1x ead-assistant permit authentication-escape** to enable support for 802.1X Auth-Fail and critical VLANs in 802.1X EAD assistant.

Use `undo dot1x ead-assistant permit authentication-escape` to restore the default.

Syntax

```
dot1x ead-assistant permit authentication-escape
undo dot1x ead-assistant permit authentication-escape
```

Default

802.1X Auth-Fail and critical VLANs cannot take effect when 802.1X EAD assistant is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to remove the EAD entries of users before it assigns the users to 802.1X Auth-Fail and critical VLANs.

Examples

```
# Enable support for 802.1X Auth-Fail and critical VLANs in 802.1X EAD assistant.
<Sysname> system-view
[Sysname] dot1x ead-assistant permit authentication-escape
```

Related commands

```
dot1x ead-assistant enable
```

Modified feature: Displaying information about online 802.1X users

Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the `display dot1x connection` command.

Command changes

Modified command: display dot1x connection

Syntax

```
display dot1x connection [ open ] [ interface interface-type
interface-number | slot slot-number | user-mac mac-address | user-name
name-string ]
```

Views

Any view

Change description

The **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display dot1x connection** command:

```
<Sysname> display dot1x connection
```

```
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```
User access state: Successful
```

```
Authentication domain: aaa
```

```
IPv4 address: 192.168.1.1
```

```
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
```

```
Authentication method: CHAP
```

```
Initial VLAN: 1
```

```
Authorization untagged VLAN: 6
```

```
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33  
                                35 37 40 to 100
```

```
Authorization VSI: N/A
```

```
Authorization ACL number/name: 3001
```

```
Authorization dynamic ACL name: N/A
```

```
Authorization user profile: N/A
```

```
Authorization CAR: N/A
```

```
Authorization URL: N/A
```

```
Termination action: Default
```

```
Session timeout period: 2 s
```

```
Online from: 2013/03/02 13:14:15
```

```
Online duration: 0h 2m 15s
```

Modified feature: Displaying information about online MAC authentication users

Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the **display mac-authentication connection** command.

Command changes

Modified command: display mac-authentication connection

Syntax

```
display mac-authentication connection [ open ] [ interface interface-type  
interface-number | slot slot-number | user-mac mac-address | user-name  
user-name ]
```

Views

Any view

Change description

The **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display mac-authentication connection** command:

```
<Sysname> display mac-authentication connection
Total connections: 1
Slot ID: 1
User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: macusers
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 2 sec
Offline detection: 100 sec (server-assigned)
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s
```

Modified feature: L2PT for CFD

Feature change description

As from this version, the device supports enabling L2TP for CFD and configuring the destination multicast MAC address for tunneled packets of the specified protocol.

Command changes

Modified command: l2protocol type tunnel-dmac

Old syntax

```
l2protocol type { cdp | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp |
pagp | pvst | stp | udld | vtp } tunnel-dmac mac-address
undo l2protocol type { cdp | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp
| pagp | pvst | stp | udld | vtp } tunnel-dmac
```

New syntax

```
l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp |  
mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac mac-address  
  
undo l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp  
| mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac
```

Views

System view

Change description

Before modification: The **cfd** keyword is not supported.

After modification: The **cfd** keyword is supported.

Modified command: l2protocol tunnel dot1q

Old syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst |  
stp | udld | vtp } tunnel dot1q  
  
undo l2protocol { cdp | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp |  
pvst | stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld | vtp }  
tunnel dot1q  
  
undo l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q
```

New syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp |  
pvst | stp | udld | vtp } tunnel dot1q  
  
undo l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp  
| pvst | stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q  
  
undo l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp  
| udld | vtp } tunnel dot1q
```

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Change description

Before modification: The **cfd** keyword is not supported.

After modification: The **cfd** keyword is supported.

Modified command: display l2protocol statistics

Syntax

```
display l2protocol statistics [ interface interface-type interface-number ]
```

Views

Any view

Change description

Before modification: The device does not support displaying L2TP statistics for CFD protocol packets.

After modification: The device supports displaying L2TP statistics for CFD protocol packets.

Display L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

```
<Sysname> display l2protocol statistics
```

L2PT statistics information on interface Bridge-Aggregation1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDP	0	3	0	0
EOAM	0	2	0	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	0	3	0	0
MVRP	0	0	0	0
PAGP	0	1	0	0
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0
CFD	0	0	0	0

L2PT statistics information on interface GigabitEthernet1/0/1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDP	2	3	3	0
EOAM	5	2	9	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	3	3	3	3
MVRP	0	0	0	0
PAGP	5	1	7	3
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0

CFD	0	0	0	0
-----	---	---	---	---

Release 6330

This release has the following changes:

- [New feature: Enabling fast PoE for a PSE](#)
- [Modified feature: L2PT for CFD and DTP](#)
- [Modified feature: Displaying information about online 802.1X users](#)
- [Modified feature: Displaying information about online MAC authentication users](#)

New feature: Enabling fast PoE for a PSE

Enabling fast PoE for a PSE

About this task

This feature enables PIs on a PSE to supply power to PDs immediately after the PSE is powered on.

Restrictions and guidelines

You must re-configure this feature if you changed other PoE settings after configuring this feature.

Procedure

1. Enter system view.
system-view
2. Enable fast PoE for a PSE.
poe fast-on enable pse *pse-id*
By default, fast PoE is disabled for a PSE.

Command reference

poe fast-on enable

Use **poe fast-on enable** to enable fast PoE for a PSE.

Use **undo poe fast-on enable** to disable fast PoE for a PSE.

Syntax

```
poe fast-on enable pse pse-id  
undo poe fast-on enable pse pse-id
```

Default

Fast PoE is disabled for a PSE.

Views

System view

Predefined user roles

network-admin

Parameters

pse *pse-id*: Specifies a PSE by its ID.

Usage guidelines

Fast PoE enables PIs on a PSE to supply power to PDs immediately after the PSE is powered on.

You must re-configure this command if you changed other PoE settings after configuring this command.

Examples

```
# Enable fast PoE for PSE 4.
```

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

```
[Sysname] poe fast-on enable pse 4
```

Modified feature: L2PT for CFD and DTP

Feature change description

As from this version, the device supports enabling L2TP for CFD and DTP and configuring the destination multicast MAC address for tunneled packets of the specified protocol.

Command changes

New command: l2protocol type tunnel-dmac

Use **l2protocol type tunnel-dmac** to set the destination multicast MAC address for tunneled packets of the specified protocol.

Use **undo l2protocol type tunnel-dmac** to restore the default.

Syntax

```
l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp |  
mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac mac-address
```

```
undo l2protocol type { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp  
| mvrp | pagp | pvst | stp | udld | vtp } tunnel-dmac
```

Default

The tunneled packets of all protocols use 010f-e200-0003 as the destination multicast MAC address.

Views

System view

Predefined user roles

network-admin

Parameters

cdp: Specifies CDP.

cfd: Specifies CFD.

dldp: Specifies DLDP.

dtp: Specifies DTP.

eoam: Specifies EOAM.

gvrp: Specifies GVRP.

lacp: Specifies LACP.

lldp: Specifies LLDP.

mvrp: Specifies MVRP.

pagp: Specifies PAgP.

pvst: Specifies PVST.

stp: Specifies STP.

udld: Specifies UDLD.

vtp: Specifies VTP.

mac-address: Specifies a destination multicast MAC address for tunneled packets of the specified protocol, in the range of 0100-0000-0000 to 01ff-ffff-ffff.

Usage guidelines

As a best practice, set different destination multicast MAC addresses on PEs connected to different customer networks. It prevents L2PT from sending packets of a customer network to another customer network.

The **l2protocol tunnel-dmac** command sets the destination multicast MAC address for tunneled packets of all protocols. This command sets the destination multicast MAC address for tunneled packets of the specified protocol. If both commands are executed, the **l2protocol type tunnel-dmac** command takes priority.

For tunneled packets to be recognized, set the same destination multicast MAC address for packets of the same protocol on PEs that are connected to the same customer network.

If you execute this command multiple times for a protocol, the most recent configuration takes effect.

Examples

Set the destination multicast MAC address to 0100-0ccd-cddc for tunneled packets of CFD.

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

```
[Sysname] l2protocol type cfd tunnel-dmac 0100-0ccd-cddc
```

Modified command: l2protocol tunnel dot1q

Old syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | dldp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst | stp |  
udld | vtp } tunnel dot1q
```

```
undo l2protocol { cdp | dldp | eoam | gvrp | lacp | lldp | mvrp | pagp | pvst |  
stp | udld | vtp } tunnel dot1q
```

In Layer 2 aggregate interface view:

```
l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld | vtp }  
tunnel dot1q
```

```
undo l2protocol { cdp | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q
```

New syntax

In Layer 2 Ethernet interface view:

```
l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp |  
pvst | stp | udld | vtp } tunnel dot1q
```

```
undo l2protocol { cdp | cfd | dldp | dtp | eoam | gvrp | lacp | lldp | mvrp | pagp  
| pvst | stp | udld | vtp } tunnel dot1q
```


In Layer 2 aggregate interface view:

```
l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp | udld  
| vtp } tunnel dot1q  
  
undo l2protocol { cdp | cfd | gvrp | lacp | lldp | mvrp | pagp | pvst | stp  
| udld | vtp } tunnel dot1q
```

Views

layer 2 Ethernet interface view

layer 2 aggregate interface view

Change description

Before modification: L2TP cannot be enabled for CFD or DTP.

After modification: L2TP can be enabled for CFD and DTP.

Modified command: display l2protocol statistics

Syntax

```
display l2protocol statistics [ interface interface-type  
interface-number ]
```

Views

Any view

Change description

Before modification: The device does not support displaying L2TP statistics for CFD or DTP protocol packets.

After modification: The device supports displaying L2TP statistics for CFD and DTP protocol packets.

Display L2PT statistics for all Layer 2 Ethernet and aggregate interfaces.

```
<Sysname> display l2protocol statistics
```

L2PT statistics information on interface Bridge-Aggregation1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
CDP	0	0	0	0
DLDP	0	3	0	0
EOAM	0	2	0	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	0	3	0	0
MVRP	0	0	0	0
PAGP	0	1	0	0
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0
CFD	0	0	0	0

L2PT statistics information on interface GigabitEthernet1/0/1:

Protocol	Encapsulated	Decapsulated	Forwarded	Dropped
----------	--------------	--------------	-----------	---------

CDP	0	0	0	0
DLDP	2	3	3	0
EOAM	5	2	9	0
GVRP	8	4	9	2
LACP	0	0	0	0
LLDP	3	3	3	3
MVRP	0	0	0	0
PAGP	5	1	7	3
PVST	0	0	0	0
STP	5	5	5	0
Tunnel	N/A	N/A	100	10
VTP	0	6	0	0
UDLD	0	0	0	0
DTP	0	0	0	0
CFD	0	0	0	0

Modified feature: Displaying information about online 802.1X users

Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the **display dot1x connection** command.

Command changes

Modified command: display dot1x connection

Syntax

```
display dot1x connection [ open ] [ interface interface-type
interface-number | slot slot-number | user-mac mac-address | user-name
name-string ]
```

Views

Any view

Change description

The **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display dot1x connection** command:

```
<Sysname> display dot1x connection
```

```
Total connections: 1
```

```
Slot ID: 1
```

```
User MAC address: 0015-e9a6-7cfe
```

```
Access interface: GigabitEthernet1/0/1
```

```
Username: ias
```

```

User access state: Successful
Authentication domain: aaa
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33
                                35 37 40 to 100

Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s

```

Modified feature: Displaying information about online MAC authentication users

Feature change description

As from this version, the **Authorization dynamic ACL name** field is added to the command output from the **display mac-authentication connection** command.

Command changes

Modified command: display mac-authentication connection

Syntax

```

display mac-authentication connection [ open ] [ interface interface-type
interface-number | slot slot-number | user-mac mac-address | user-name
user-name ]

```

Views

Any view

Change description

The **Authorization dynamic ACL name** field was added to the command output from this command. If no dynamic ACL is assigned, this field displays **N/A**. If a dynamic ACL is assigned but the assignment fails, this field displays **(NOT effective)** next to the dynamic ACL name.

The following is a sample output from the **display mac-authentication connection** command:

```

<Sysname> display mac-authentication connection
Total connections: 1
Slot ID: 1

```

User MAC address: 0015-e9a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
User access state: Successful
Authentication domain: macusers
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization VSI: N/A
Authorization ACL number/name: 3001
Authorization dynamic ACL name: N/A
Authorization user profile: N/A
Authorization CAR: N/A
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 2 sec
Offline detection: 100 sec (server-assigned)
Online from: 2013/03/02 13:14:15
Online duration: 0h 2m 15s