Hewlett Packard
Enterprise

HPE HSR6602-CMW710-R7103P09 Release Notes

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

Contents

List of Tables

This document describes the features, restrictions and guidelines, open problems, and workarounds for version HPE HSR6602-CMW710-R7103P09. Before you use this version in a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HPE HSR6602-CMW710-R7103P09 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Important information

In this software the format of the configuration files has been changed. To avoid any problems downgrading software, please backup the configuration file before upgrading. More details may be found in the Open problems and workarounds section "Open problems and workarounds."

Version information

Version number

Comware software, Version 7.1.054, Release 7103P09

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

Version history

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
CMW710-R7103P09	CMW710-R7103P08	2016-5-10	Release version	Fixes bugs
CMW710-R7103P08	CMW710-R7103P07	2016-3-10	Release version	Fixes bugs
CMW710-R7103P07	CMW710-R7103P06	2016-1-28	Release version	Fixes bugs
CMW710-R7103P06	CMW710-R7103P05	2015-12-16	Release version	Fixes bugs
CMW710-R7103P05	CMW710-R7103	2015-10-14	Release version	Fixes bugs
CMW710-R7103	None	2015-2-13	Release version	N/A

Hardware and software compatibility matrix

△ **CAUTION:**

To avoid an upgrade failure, verify the hardware and software compatibility before performing an upgrade.

Table 2 Hardware and software compatibility matrix 1

Item	Specifications
Product family	HSR6600 series
Hardware platform	HSR6602-G/HSR6602-XG
Memory	HSR6602-G: 2 GB/4 GB HSR6602-XG: 4 GB

Flash/CF Card	512 MB (minimum)
Boot ROM version	2.04
Host software	HSR6602-CMW710-R7103P09.ipe – requires JG353A HP HSR6602-G Router, JG354A HP HSR6602-XG Router, JG776A HP HSR6602-G TAA-compliant Router or JG777A HP HSR6602-XG TAA-compliant Router
Software image file	HSR6602-CMW710-R7103P09.ipe
iMC version	iMC EAD 7.1 (E0301P03) iMC TAM 7.1 (E0302P08) iMC UAM 7.1 (E0302P08) iMC IVM 7.1 (E0301P01) iMC MVM 7.1 (E0301) iMC NTA 7.1 (E0301P04) iMC PLAT 7.1 (E0303P16) iMC RAM 7.1 (E0301P04) iMC SHM 7.1 (E0301P02) iMC UBA 7.1 (E0301P04)
iNode	iNode PC 7.1 (E0307)

Table 3 Hardware and software compatibility matrix 2

Board model	Board version	Logic version	Remarks
HSR6602-G	VER.A	Basic: 100 Extended: 200	HPE FlexNetwork HSR6602 G Router
HSR6602-XG	VER.A	Basic: 100 Extended: 200	HPE FlexNetwork HSR6602 XG Router
FIP-20	VER.A	100	HPE FlexNetwork 6600 FIP-20 Flexible Interface Platform Router Module
HIM-8FE	VER.B	100	HPE FlexNetwork 6600 8-port 10/100BASE-T HIM Module
HIM-4GBE	VER.B	200	HPE FlexNetwork 6600 4GbE WAN HIM Router Module
HIM-4GBP	VER.A	200	HPE FlexNetwork 6600 4-port GbE SFP HIM Router Module
HIM-8GBE	VER.B	200	HPE FlexNetwork 6600 8GbE WAN HIM Router Module
HIM-8GBP	VER.A	200	HPE FlexNetwork 6600 8-port GbE SFP HIM Router Module
HIM-1EXP	VER.A	200	HPE FlexNetwork 6600 1-port 10GbE XFP HIM Router Module
HIM-CL1P	VER.B	Main card: 100 Subcard: 200	HPE FlexNetwork 6600 1-port OC-3 (E1/T1) CPOS HIM Router Module
HIM-CL2P	VER.B	Main card: 100 Subcard: 200	HPE FlexNetwork 6600 2-port OC-3 E1/T1 CPOS HIM Router Module
HIM-CLS1P	VER.A	100	HP A6600 1-port OC-3/STM-1 (E3/T3) CPOS SFP HIM Module

HIM-CLS2P	VER.A	100	HP A6600 2-port OC-3/STM-1 (E3/T3) CPOS SFP HIM Module
HIM-MSP2P	VER.A	100	HPE FlexNetwork 6600 2-port OC-3/1-port OC-12 POS HIM Router Module
HIM-MSP4P	VER.A	100	HPE FlexNetwork 6600 4-port OC-3/2-port OC-12 POS HIM Router Module
HIM-PS1P	VER.A	100	HPE FlexNetwork 6600 1-port OC-48/STM-16 POS (SFP) Router Module
HIM-TS8P	VER.A	200	HPE FlexNetwork 6600 8-port OC-3c/OC-12c POS/GbE SFP HIM Module
HIM-16GBP	VER.A	100	HPE FlexNetwork HSR6800 16-port GbE SFP HIM Module
HIM-2EXP	VER.A	100	HPE FlexNetwork HSR6800 2-port 10GbE SFP+ HIM Module
MIM-8E1	VER.B	100	HP A-MSR 8-port E1/CE1/PRI (75ohm) MIM Module
MIM-8E1-F	VER.B	100	HP A-MSR 8-port E1/Fractional E1 (75ohm) MIM Module
RT-MIM-1CT3-V2-H3	VER.A	100	HP A-MSR 1-Port FT3/CT3 MIM Module

To display the host software and BootWare version, use the following command:

```
<HPE>display version
HPE Comware Software, Version 7.1.054, Release 7103P09                 ------- Note①
Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP
HPE HSR6602-XG uptime is 2 weeks, 5 days, 23 hours, 22 minutes
Last reboot reason : Power on
Boot image: flash:/SR6602X-CMW710-BOOT-R7103P09.bin
Boot image version: 7.1.054, Release 7103P09
  Compiled Apr 19 2016 16:00:01
System image: flash:/SR6602X-CMW710-SYSTEM-R7103P09.bin
System image version: 7.1.054, Release 7103P09
  Compiled Apr 19 2016 16:00:01

Slot 0: HSR6602-XG uptime is 0 week, 1 day, 2 hours, 48 minutes
 CPU type: FREESCALE P4080 1500MHz
 4096M bytes DDR3 SDRAM Memory
 8M bytes Flash Memory
 128K bytes NVRAM
 PCB              Version: Ver.A
 Basic      Logic Version: 1.0
 Extend     Logic Version: 2.0
 Basic   BootWare Version: 2.04                                  ------note②
 Extend  BootWare Version: 2.04                                  ------note②
 [FIXED PORTS] MGE              (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
```

```
[FIXED PORTS] Combo 4GE        (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
[FIXED PORTS] 2XGE             (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
```

Upgrading restrictions and guidelines

HSR6602 routers that use CMW520 cannot load this software image file directly. You can upgrade an HSR6602 router from Comware V5 to Comware V7 (see *HSR6600_HSR6800 Comware V5-V7 Migration Guide(5998-7251)*).

Hardware feature updates

CMW710-R7103P09

This version supports the new hardware: RT-MIM-1CT3-V2-H3 (1-Port T3/CT3/FT3 MIM Interface Module MIM-1CT3-V2).

For supported modules, see Table 6.

CMW710-R7103P08

None.

CMW710-R7103P07

None.

CMW710-R7103P06

None.

CMW710-R7103P05

None.

CMW710-R7103

This code does not support HP 6600 FIP-10 Flexible Interface Platform Router Module.

This code does not support USB port.

Software feature and command updates

See *HPE HSR6602-CMW710-R7103P09 Release Notes (Software Feature Changes)*.

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
CMW710-R7103P09			
New	None	None	None
Modified	None	None	None
CMW710-R7103P08			
New	None	None	None
Modified	None	None	None
CMW710-R7103P07			
New	hh3cIfTable	HH3C-IF-EXT-MIB	As per MIB
Modified	None	None	None
CMW710-R7103P06			
New	Scalar objects hh3cSnmpExtCommunityTable	HH3C-SNMP-EXT-MIB	As per MIB
	hh3cVsiScalarGroup hh3cVsiPwBindTable hh3cVsiFloodMacTable hh3cVsiLocalMacTable hh3cVsiNextAvailableVsiIfID	HH3C-VSI-MIB	As per MIB
Modified	None	None	None
CMW710-R7103P05			
New	hh3cIpRanDcnMAC hh3cIpRanDcnVendor hh3cIpRanDcnNeInfoMAC hh3cIpRanDcnNeInfoVendor	HH3C-IPRAN-DCN-MIB	As per MIB
	hh3cEntityExtSFPAlarmOnEx hh3cEntityExtSFPAlarmOffEx	HH3C-ENTITY-EXT-MIB	As per MIB
	HH3C-L2VPN-MIB	HH3C-L2VPN-MIB	As per MIB
Modified	None	None	None
CMW710-R7103			
New	None	None	None
Modified	None	None	None

Operation changes

Operation changes in CMW710-R7103P07

The operation of downgrading software from Comware V7 to Comware V5 is changed.

Before modification, you can follow these steps to downgrade software to Comware V5:

1. Use a Comware V5 BootWare conversion image to downgrade the BootWare.
2. Load a Comware V5 software image to complete the downgrade.

After modification, you must firstly downgrade the software version to R7153P06 or an earlier version before you use the previous downgrade method. Otherwise, the error "Something wrong with the file" occurs.

You can also follow these steps to downgrade software to Comware V5:

3. Use a Comware V5 software image to downgrade the BootWare.
4. Load a Comware V5 software image to complete the downgrade.

The following example shows how to use this method to downgrade to Comware V5.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4): 4
==========================<ETHERNET PARAMETER SET>==========================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|         Ctrl+D = Quit.                                                    |
============================================================================
Protocol (FTP or TFTP) :ftp
Load File Name          :HSR6602_Bootware_V7.btw
                        :HSR6602_MCP-CMW520-R3303P27.bin   // Load a Comware V5 software
image
Target File Name        :HSR6602_Bootware_V7.btw
                        :HSR6602_MCP-CMW520-R3303P27.bin  // Load a Comware V5 software
image
Server IP Address       :192.168.2.114
Local IP Address        :192.168.2.109
Subnet Mask             :0.0.0.0
Gateway IP Address      :0.0.0.0
FTP User Name           :1
FTP User Password       :*
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                   |
|<2> Update Extended BootWare                                               |
|<3> Update Basic BootWare                                                  |
|<4> Modify Ethernet Parameter                                              |
|<0> Exit To Main Menu                                                      |
============================================================================
Enter your choice(0-4): 1
Loading.....................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
......................................Done.
125939712 bytes downloaded!
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare...............Done.
Updating Extended BootWare? [Y/N]Y
Updating Extended BootWare..........Done.
```

Operation changes in CMW710-R7103P06

Modified the display names of cards and subcards

The names displayed for the following cards and subcards are modified to be the same as their marks:

Original name	New name
HIM-8GBE	8GBE
HIM-8FE	8FE
HIM-4GBE	4GBE
HIM-4GBP	4GBP
HIM-8GBP	8GBP
HIM-1EXP	1EXP
HIM-MSP4P(OC-3)	MSP4P
HIM-MSP4P(OC-12)	MSP4P

HIM-PS1P(OC-48)	PS1P
HIM-MSP2P(OC-3)	MSP2P
HIM-MSP2P(OC-12)	MSP2P
HIM-PS1P(ECPOS)	PS1P
HIM-TS8P	TS8P
HIM-4G4P	4G4P
HIM-8GBP-V2	8GBP-V2
HIM-2EXP	RT-HIM-2EXP
HIM-16GBP	RT-HIM-16GBP
HIM-CL2P(E)	CL2P
HIM-CL2P(T)	CL2P
HIM-CL1P(E)	CL1P
HIM-CL1P(T)	CL1P
HIM-CLS2P(E)	CLS2P
HIM-CLS2P(T)	CLS2P
HIM-CLS2P(OC-3)	CLS2P
HIM-CLS1P(E)	CLS1P
HIM-CLS1P(T)	CLS1P
HIM-CLS1P(OC-3)	CLS1P
MIM-8E1(75)	8E1(75)
MIM-8E1_F(75)	8E1(75)-F
MIM-8T1	8T1
MIM-8T1_F	8T1-F
HIM-AL1P	AL1P
HIM-AL2P	AL2P
MIM-8SAE-V2	8SAE-V2
MIM-4SAE-V2	4SAE-V2
MIM-2SAE-V2	2SAE-V2
MIM-8SAE	8SAE
MIM-4SAE	4SAE
MIM-2SAE	2SAE
MIM-2GBE	2GBE
RPE-X3	RT-RPE-X3
SAP-28GE	RT-SAP-28GE
SAP-20GE2XP	RT-SAP-20GE2XP
SFE-L1	RT-SFE-L1

Changed the operations performed on cards that reach the shutdown temperature threshold

Before modification, the system generates a warning and powers off a card when the temperature of the card reaches the shutdown temperature threshold.

After modification, the system only generates a warning when the shutdown temperature threshold of a card is reached.

The output from the **display environment** command was also modified.

- Before modification, the value of the **ShutdownLimit** field can be equal to or lower than 100.

```
[HPE]display environment
System temperature information (degree centigrade):
------------------------------------------------------------------------------
Slot   Sensor    Temperature LowerLimit WarningLimit AlarmLimit ShutdownLimit
Vent   Hotspot 1 36          0          120          255        255
1      Outflow 1 39          0          54           58         255
1      Hotspot 1 47          0          72           77         255
2      Inflow  1 38          0          59           74         79
2      Outflow 1 40          0          65           70         75
2      Hotspot 1 52          0          68           73         78
3      Inflow  1 34          0          50           60         70
3      Outflow 1 38          0          55           65         75
3      Hotspot 1 45          0          80           90         100
4      Inflow  1 34          0          62           66         71
4      Outflow 1 45          0          66           79         84
4      Hotspot 1 45          0          66           79         84
```

- After modification, the value of the **ShutdownLimit** field can only be 255.

```
[HPE]display environment
System temperature information (degree centigrade):
------------------------------------------------------------------------------
Slot   Sensor    Temperature LowerLimit WarningLimit AlarmLimit ShutdownLimit
Vent   Hotspot 1 36          0          120          255        255
1      Outflow 1 39          0          54           58         255
1      Hotspot 1 47          0          72           77         255
2      Inflow  1 38          0          59           74         255
2      Outflow 1 40          0          65           70         255
2      Hotspot 1 52          0          68           73         255
3      Inflow  1 34          0          50           60         255
3      Outflow 1 38          0          55           65         255
3      Hotspot 1 45          0          80           90         255
4      Inflow  1 34          0          62           66         255
4      Outflow 1 45          0          66           79         255
4      Hotspot 1 45          0          66           79         255
```

Changed the order of banners for SSH login

This version changed the order of banners for SSH login. This modification does not affect SSH authentication, and banner display for SSH login supports only SSH2.0.

Old order	Username	Password	Copyright statement	Legal banner	MOTD banner	Login banner	Shell banner
New order	Username	Login banner	Password	Copyright statement	Legal banner	MOTD banner	Shell banner

Open problems and workarounds

None.

List of resolved problems

Resolved problems in CMW710-R7103P09

201601210277

- Symptom: L2TP users cannot come online.
- Condition: This symptom occurs when the device acts as the LNS and the remote DHCP server uses only BOOTP packets to respond to requests.

201603020564

- Symptom: Packets are lost during a master/subordinate switchover.
- Condition: This symptom occurs when the device is installed with two RPE-X3 MPUs.

201603100643

- Symptom: In an SR6602-X IRF fabric, information about interfaces on an interface module of a subordinate device cannot be displayed by using the **display interface** command.
- Condition: This symptom occurs after the interface module is removed from and then installed in the subordinate device.

201603100660

- Symptom: In an SR6602-X IRF fabric, information about interfaces on a removed interface module can still be displayed by using the **display interface** command.
- Condition: This symptom occurs after the interface module is removed from a subordinate device in the SR6602-X IRF fabric.

201603160076

- Symptom: The IPsec service is interrupted.
- Condition: This symptom might occur when the device tries to establish an IPsec connection with the peer.

201603220523

- Symptom: The network management software cannot obtain the QoS policy applied to an interface.
- Condition: This symptom might occur if two QoS policies are applied to interfaces and one of the QoS policies is removed.

201603230029

- Symptom: In an SR6602-X IRF fabric, a subordinate device hangs up when loading software images.

- Condition: This symptom occurs after you use the **boot-loader file** *flash:/SR6602X.ipe* **all main** command to specify startup images.

201603300017

- Symptom: CVE-2015-3195
- Condition: Fixed vulnerability with malformed OpenSSL X509_ATTRIBUTE structure used by the PKCS#7 and CMS routines which may cause memory leak.
- Symptom: CVE-2015-3196
- Condition: Fixed vulnerability where a race condition can occur when specific PSK identity hints are received.

201604120031

- Symptom: The MPU of the device reboots unexpectedly.
- Condition: This symptom might occur if the BGP peer of the device is repeatedly enabled and disabled to exchange labeled routes with the device in BGP IPv4 unicast address family view.

201604140598

- Symptom: MPLS traffic cannot be forwarded when the device works with a Huawei device.
- Condition: This symptom might occur if the device is configured with MPLS and routing entries are repeatedly created and deleted.

201604180487

- Symptom: Packets are lost after NetStream is enabled on a FIP-600 LPU.
- Condition: This symptom occurs when the following conditions are met:
  - NetStream is enabled on interfaces of the FIP-600 LPU by using the **ip netstream** command.
  - TCP FIN or RST packets and other types of packets exist on the device.

201604190108

- Symptom: The MPU and LPUs reboot unexpectedly in an inter-AS option C MPLS L3VPN with equal cost LSPs.
- Condition: This symptom occurs when the P device is enabled and then disabled with the MPLS label forwarding statistics for all LSPs.

201604140598

- Symptom: SSH users cannot log in to the device through a Cygwin client.
- Condition: This symptom might occur when SSH users log in to the device through a Cygwin client.

Resolved problems in CMW710-R7103P08

201601210277

- Symptom: An aggregate interface cannot forward traffic.
- Condition: This symptom might occur if the following conditions exist:
  - Aggregation member ports reside on an HSR6602 router.
  - VRRP is configured on the aggregate interface and then the configuration is cancelled.

201601290376

- Symptom: An L2TP dialup user fails to log in.
- Condition: This symptom occurs if the following conditions exist:

    - The router acts as the LNS.
    - The value of the **idle-timeout** attribute that the RADIUS server assigns is zero after the user dials up.

201602010183

- Symptom: A large number of packets are lost on the interface connected to an MP-group interface.
- Condition: This symptom occurs if the MP-group interface is configured with CBQ and the MP-group interface is congested.

201602030218

- Symptom: Configurations of the **filter-policy import** and **filter-policy export** commands in RIP view are lost after the router is rebooted to complete software upgrade.
- Condition: This symptom occurs after the router is rebooted to complete software upgrade.

Resolved problems in CMW710-R7103P07

201601040581

- Symptom: The network management software does not receive an inform message when an interface goes down.
- Condition: This symptom might occur if the interface is on the active link between the device and the PC where the network management software resides.

201601060147

- Symptom: The CPU usage is high.
- Condition: This symptom occurs if one of the following conditions exists:
    - The **display cpu-usage** command is executed to display the current CPU usage statistics.
    - The **display cpu-usage history** command is executed to display the historical CPU usage statistics in a coordinate system.

201601120290

- Symptom: The device cannot operate correctly and LPUs reboot repeatedly.
- Condition: This symptom might occur if LDP neighbor flapping or route flapping occurs in MPLS L3VPN inter-AS option C.

201511140047

- Symptom: The network management software fails to obtain the complete description of an interface.
- Condition: This symptom occurs if the description of the interface has more than 64 characters.

201601050452

- Symptom: A Telnet user fails to log in the HSR6600 device in an IRF fabric.
- Condition: This symptom occurs after a master/subordinate switchover.

201512010185

- Symptom: CVE-2015-7871
- Condition: Cause ntpd to accept time from unauthenticated peers.
- Symptom: CVE-2015-7704

- Condition: An ntpd client forged by a DDoS attacker located anywhere on the Internet, that can exploit NTP's to disable NTP at a victim client or it may also trigger a firewall block for packets from the target machine.
- Symptom: CVE-2015-7705
- Condition: The DDoS attacker can send a device a high volume of ntpd queries that are spoofed to look like they come from the client. The servers then start rate-limiting the client.
- Symptom: CVE-2015-7855
- Condition: Ntpd mode 6 or mode 7 packet containing an unusually long data value could possibly use cause NTP to crash, resulting in a denial of service.

Resolved problems in CMW710-R7103P06

201502130111

- Symptom: The router acts as an LNS to work with a ZTE LAC. If an L2TP user fails authentication, the L2TP tunnel for the user is removed, and all L2TP sessions on the tunnel are cleared.
- Condition: This symptom might occur if the router acts as an LNS to work with a ZTE LAC, and an L2TP user fails authentication.

201507020208

- Symptom: An LPU that hosts an MP-group interface reboots or PPP commands become unavailable if member interfaces are frequently added and removed for the MP-group interface and traffic on the interface exceeds its bandwidth.
- Condition: This symptom might occur if member interfaces are frequently added and removed for an MP-group interface, and traffic on the interface exceeds its bandwidth.

201507140365

- Symptom: A GE copper interface on a FIP-300 or FIP-310 module cannot forward packets.
- Condition: This symptom might occur if the GE copper interface is operating at 100 Mbps.

201510140192

- Symptom: The subordinate routers of an IRF fabric reboot constantly if the router joins the IRF fabric by using a SAP-28GE card for IRF connection.
- Condition: This symptom might occur if the router joins an IRF fabric by using a SAP-28GE card for IRF connection.

201510160288

- Symptom: On an IRF fabric, some IPsec policy settings are lost after a master/subordinate switchover.
- Condition: This symptom might occur if more than 1024 IPsec policies are configured on the IRF fabric, and a master/subordinate switchover occurs after the configuration is saved.

201511100405

- Symptom: If the router or its peer uses a HIM-CL1P or HIM-CL2P subcard for interconnection, link flapping occurs.
- Condition: This symptom might occur if the subcard uses the default operating mode, and the **e1 channel-set** command is executed on the subcard.

201511120549

- Symptom: Users cannot pass authentication because the format of the Calling-Station-Id attribute in RADIUS packets sent by the router is incorrect.

- Condition: This symptom might occur if the format of the Calling-Station-Id attribute in RADIUS packets sent by the router is incorrect.

201512100032

- Symptom: The router cannot communicate with an MSR3600 router through an aggregate interface.
- Condition: This symptom might occur if one of the following conditions exists:
    - A SAP-28GE card provides aggregation member interfaces, and the IDs of the interfaces are in the range of both 0 to 15 and 16 to 27.
    - A SAP-20GE2XP card provides aggregation member interfaces, and the IDs of the interfaces are in the range of both 0 to 15 and 16 to 19.

Resolved problems in CMW710-R7103P05

201508290045

- Symptom: The CPU usage is high when Telnet is used to log in to the router.
- Condition: This symptom occurs if the login page is closed unexpectedly or login attempts are made repeatedly.

201505250253

- Symptom: A router crashes when it processes a large number of packets.
- Condition: This symptom might occur if the packets are all destined to interfaces on the router.

201509240204

- Symptom: All FIP-600 modules on a router reboot unexpectedly.
- Condition: This symptom occurs when a large number of LSPs are configured and deleted repeatedly on the router.

201504150287

- Symptom: CVE-2015-0209
- Condition: A malformed EC private key file consumed via the d2i_ECPrivateKey function could cause a use after free condition. This could lead to a DoS attack or memory corruption for applications that receive EC private keys from untrusted sources.

- Symptom: CVE-2015-0287
- Condition: Reusing a structure in ASN.1 parsing may allow an attacker to cause memory corruption via an invalid write. Applications that parse structures containing CHOICE or ANY DEFINED BY components may be affected.

- Symptom: CVE-2015-0288
- Condition: The function X509_to_X509_REQ will crash with a NULL pointer dereference if the certificate key is invalid.

- Symptom: CVE-2015-0289
- Condition: The PKCS#7 parsing code does not handle missing outer ContentInfo correctly. An attacker can craft malformed ASN.1-encoded PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

201508190167

- Symptom: An MP-group interface cannot forward packets after it is shut down and then brought up.
- Condition: This symptom occurs if the MP-group interface has a large number of member ports.

201509210156

- Symptom: In an IP RAN network, the router broadcasts DHCP-OFFER and DHCP-ACK messages to all clients.
- Condition: This symptom occurs if the router acts as a DHCP relay agent.

201508140092

- Symptom: All data packets forwarded by a Layer 3 Ethernet interface on a FIP-600 module are sent to the CPU.
- Condition: This symptom occurs after an IPsec policy is applied to and then removed from the Layer 3 Ethernet interface.

201509160316

- Symptom: Some IS-IS routes cannot be learned because 261-byte IS-IS packets are dropped.
- Condition: This symptom occurs if the HIM-16GBP subcard receives 261-byte IS-IS packets.

201509210482

- Symptom: All FIP-600 modules on the router reboot when the **display diagnostic-information** command is executed.
- Condition: This symptom occurs if the **display diagnostic-information** command is executed.

201509070246

- Symptom: In an MPLS L3VPN or MPLS L2VPN, a FIP-600 module drops VPN packets destined to the connected CE that are larger than 2088 bytes.
- Condition: This symptom occurs if the FIP-600 module connects to the CE through a Layer 3 aggregate interface.

201507160261

- Symptom: CVE-2014-8176
- Condition: If a DTLS peer receives application data between the ChangeCipherSpec and Finished messages, a segmentation fault or potentially, memory corruption might occur.

- Symptom: CVE-2015-1788
- Condition: When processing an ECParameters structure OpenSSL enters an infinite loop. This can be used to perform denial of service against any system which processes public keys, certificate requests or certificates.

- Symptom: CVE-2015-1789
- Condition: X509_cmp_time does not properly check the length of the ASN1_TIME string and/or accepts an arbitrary number of fractional seconds in the time string. An attacker can use this to craft malformed certificates and CRLs of various sizes and potentially cause a segmentation fault, resulting in a DoS on applications that verify certificates or CRLs.

- Symptom: CVE-2015-1790

- Condition: The PKCS#7 parsing code does not handle missing inner EncryptedContent correctly. An attacker can craft malformed PKCS#7 blobs with missing content and trigger a NULL pointer dereference on parsing.

- Symptom: CVE-2015-1791
- Condition: If a NewSessionTicket is received by a multi-threaded client when attempting to reuse a previous ticket then a race condition can occur potentially leading to a double free of the ticket data.

- Symptom: CVE-2015-1792
- Condition: When verifying a signedData message the CMS code can enter an infinite loop. This can be used to perform denial of service against any system which verifies signedData messages using the CMS code.

201508210327

- Symptom: A customer-facing Layer 2 Ethernet interface in a Layer 2 aggregation group cannot learn MAC addresses in an extended VLAN after the interface is removed from the Layer 2 aggregation group.
- Condition: This symptom occurs if both the Layer 2 Ethernet interface and the Layer 2 aggregate interface are assigned to the extended VLAN.

201508170311

- Symptom: An interface on the HIM-2EXP subcard cannot forward MPLS L2VPN packets.
- Condition: This symptom occurs if the interface is both configured as a member port of a Layer 3 aggregation group and used as an AC interface in an MPLS L2VPN.

201510170029

- Symptom: One or more LPUs on IRF member device 1 cannot start when the IRF fabric is restarted.
- Condition: This symptom occurs if IRF member device 1 uses the switching fabric module SFE-L1 and has an MPU in slot 0.

201510210231

- Symptom: OSPF LSAs of a router are in abnormal status, and OSPF neighbors of the router cannot learn its routing information.
- Condition: This symptom occurs when the router continuously runs for seven months.

201506190154

- Symptom: The router does not preferentially use static address allocation when receiving a DHCP-INFORM message from a client.
- Condition: This symptom occurs if the following conditions exist:
  - The client is bound to an IP address in a DHCP address pool.
  - Another DHCP address pool includes the IP address bound to the client.

201506220007(CVE-2015-5434)

- Symptom: An interface incorrectly forwards MPLS-labeled packets to the next LSRs based on LFIB entries.
- Condition: This symptom occurs when the interface does not have MPLS enabled and the interface receives MPLS-labeled packet that match the LFIB entries.

201504230025

- Symptom: The router learns an invalid ARP entry for an incoming ARP request (creates an ARP entry based on the target IP address and sender MAC address of the ARP request).
- Condition: This symptom occurs if the ARP request has a sender IP address of 0.0.0.0.

201407090600

- Symptom: The **display dcn ne-info** command executed on a router does not display the total number of online NEs on the DCN network.
- Condition: This symptom occurs if the following conditions exist:
  - The router has the largest NE ID.
  - The **display dcn ne-info** command is executed after the **silent-interface all** command is configured on the router.

201508310428

- Symptom: Some IS-IS routes cannot be learned because IS-IS packets smaller than 32 bytes are dropped.
- Condition: This symptom occurs if the HIM-16GBP or HIM-2EXP subcard receives IS-IS packets smaller than 32 bytes.

201506220012

- Symptom: CVE-2015-3143
- Condition: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request.

- Symptom: CVE-2015-3148
- Condition: cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.

201506230376

- Symptom: CVE-2015-1799
- Condition: Authentication doesn't protect symmetric associations against DoS attacks.

201504080104

- Symptom: In a VPLS network, the router forwards packets received on an AC interface out of the AC interface.
- Condition: This symptom occurs if the router learns a MAC address on the AC interface and then learns the same MAC address on the backup PW.

201504220074

- Symptom: In a VPLS network, the router forwards packets received on an AC interface out of the AC interface.
- Condition: This symptom occurs if the router learns a MAC address on the AC interface and then learns the same MAC address on the backup PW.

201502050116

- Symptom: Packets on an aggregate interface cannot be forwarded.
- Condition: This symptom occurs a period of time after you execute the **shutdown** and **undo shutdown** command sequence repeatedly on a member port of the aggregate interface.

201411120247

- Symptom: The CBQ configuration on a FIP-600 module becomes invalid after the rate limit feature is configured on the FIP-600 module.
- Condition: This symptom occurs if you configure CBQ and then configure the rate limit feature on the FIP-600 module.

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:

- HSR6600 Routers Command References(V7)
- HSR6600 Routers Configuration Guides(V7)

Documentation feedback

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

Appendix A Feature list

Hardware features

Table 5 Hardware features

Item	HSR6602-G(JG353A)	HSR6602-XG(JG354A)
Fixed ports	4 GE combo interfaces	4 GE combo interfaces and two 10GE(SFP+) ports
Slot	One slot that supports FIP-20(JG358A)	
Service module slots	FIP-20(JG358A) supports two HIM/MIM slots.	
Memory	2 GB by default; supports up to 4 GB	4 GB by default; supports up to 4 GB
Flash	8 MB	
USB port	1	
AUX port	1	
Console port	1	
Management Ethernet port	1	
Dimensions (H × W × D)	88 × 440 × 480 mm (3.46 × 17.32 × 18.90 in)	
Weight	12.1 kg (26.68 lb)	
Rated voltage range	AC input: 100 VAC to 240 VAC, 50/60 Hz DC input: –48 VDC to –60 VDC	
Max. power consumption	160 W	
Operating temperature	0°C to 45°C (32°F to 113°F)	
Operating humidity	5% to 95% (noncondensing)	
Altitude	–60 m to +4 km (–196.85 ft to +13123.36 ft)	

Table 6 Hardware features-Supported module

Item	Module	
Supported module	JG358A	HPE FlexNetwork 6600 FIP-20 Flexible Interface Platform Router Module
	JC163A	HPE FlexNetwork 6600 4GbE WAN HIM Router Module
	JC164A	HPE FlexNetwork 6600 8GbE WAN HIM Router Module
	JC171A	HPE FlexNetwork 6600 4-port GbE SFP HIM Router Module
	JC174A	HPE FlexNetwork 6600 8-port GbE SFP HIM Router Module
	JC575A	HPE FlexNetwork 6600 8-port 10/100BASE-T HIM Module
	JC168A	HPE FlexNetwork 6600 1-port 10GbE XFP HIM Router Module
	JC169A	HP A6600 2-port OC-3/STM-1 (E3/T3) CPOS SFP HIM Module
	JC170A	HP A6600 1-port OC-3/STM-1 (E3/T3) CPOS SFP HIM Module
	JC161A	HPE FlexNetwork 6600 1-port OC-3 (E1/T1) CPOS HIM Router Module

Item	Module
	JC162A HPE FlexNetwork 6600 2-port OC-3 E1/T1 CPOS HIM Router Module
	JC494A HPE FlexNetwork 6600 1-port OC-48/STM-16 POS (SFP) Router Module
	JC172A HPE FlexNetwork 6600 4-port OC-3/2-port OC-12 POS HIM Router Module
	JC173A HPE FlexNetwork 6600 2-port OC-3/1-port OC-12 POS HIM Router Module
	JC495A HP A6600 2-port OC-3c/STM-1c ATM SFP HIM Module
	JC175A HP A6600 1-port OC-3c/STM-1c ATM SFP HIM Module
	JH142A HPE FlexNetwork HSR6800 16-port GbE SFP HIM Module
	JH143A HPE FlexNetwork HSR6800 2-port 10GbE SFP+ HIM Module
	JG673A HPE FlexNetwork 6600 8-port OC-3c/OC-12c POS/GbE SFP HIM Module
	JD628A HP 1-Port FT3/CT3 MIM A-MSR Module
	JD540A HP A-MSR 2-port Enhanced Sync/Async Serial MIM Module
	JD541A HP A-MSR 4-port Enhanced Sync/Async Serial MIM Module
	JD552A HP A-MSR 8-port Enhanced Sync/Async Serial MIM Module
	JD563A HP A-MSR 8-port E1/CE1/PRI (75ohm) MIM Module
	JF255A HP A-MSR 8-port E1/Fractional E1 (75ohm) MIM Module
	JC160A HP A-MSR 8-port T1/CT1/PRI MIM Module
	JC159A HP A-MSR 8-port T1/Fractional T1 MIM Module

Software features

Table 7 Software features

Feature	Description
Layer 2 protocol	• Dynamic and static ARP • Proxy ARP • ARP for multicast • Gratuitous ARP • Ethernet, sub-interface VLAN • ETH-Trunk • QinQ termination • PPPoE server • PPP • Hardware MP in CL2P/CL1P, and software MP in other modules • FR • MFR • FR switching • HDLC • POS trunk • LLDP for Layer 3 interfaces • ATM: IPoA, PPPoA server, IPoEoA, PPPoEoA server
IP services	• TCP, UDP, IP Option, IP unnumbered • Policy routing • Layer 3 interface binding • POS interface binding

IP routing	• Static routing • Dynamic routing protocols: RIPv1/v2, OSPFv2, BGP, and IS-IS • Route recursion • Routing policy • ECMP • UCMP • BGP GTSM • ISIS MTR
IPv4 multicast	• IGMPv1/v2/v3 • PIM-DM, PIM-SM, PIM-SSM • MSDP • MBGP • Multicast static routes • Host tracking
IP applications	• DHCP Server/Relay/Client • DNS Client • NTP Server/Client • Telnet Server/Client • TFTP Client • FTP Server/Client • UDP Helper
IPv6	• Basic functions: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL, DHCPv6 Server/Proxy • IPv6 tunnel: manually configured IPv6 tunnel, IPv6-over-IPv4, GRE tunnel, automatic IPv6 over IPv4 tunnel, 6to4 tunnel, ISATAP tunnel, 6PE • 6VPE (IPv6 MPLS L3VPN) • Static routing • Dynamic routing protocols: RIPng, OSPFv3, IS-ISv6, BGP4+ • IPv6 multicast protocols: MLDv1/v2, PIM6-DM, PIM6-SM, PIM6-SSM
QoS	• Traffic classification: based on port, MAC address, IP address, IP priority, DSCP priority, TCP/UDP port number, and protocol type • Traffic policing: CAR rate limiting, granularity configurable • Rate limiting based on source/destination address (supporting subnet-based rate limiting) • GTS • Priority Mark/Remark • Queue scheduling mechanism: FIFO, PQ, CQ, WFQ, RTPQ, CBWFQ • Congestion avoidance algorithm: tail drop, WRED • Rate limit • MPLS QoS • IPv6 QoS • H-QoS • QPPB
Security	• ACL • ACL acceleration • Time-based access control • Packet filter firewall • ASPF • TCP attack prevention on local host • Control panel rate limiting • Virtual defragment reassembly

	• URPF • Hierarchical user management and password protection • AAA • RADIUS • TACACS • Portal authentication (supporting collaboration with EAD, portal authentication bypass) • PKI • SSH 1.5/2.0 • RSA • IPSec, IPSec for VPNs, IKE • BGP/BGP4+ support for GTSM • Password control
Special service	• NAT, NAT for VPNs, VPN NAT, NAT session log • Connection limit • GRE tunnel (supporting point to multi-point applications) • IPSec tunnel and IPSec multiple instances • L2TP • NetStream (supporting v5/v8/v9 packet frames; supporting IPv4, IPv6 and MPLS packets) • ADVPN (Auto Discovery VPN)
MPLS	• L3VPN: Inter-domain MPLS VPN (Option1/2/3), nested MPLS VPN, Hierarchy PE (HoPE), CE dual homing, MCE, multi-role host • L2VPN: VPLS, Martini, Kompella, CCC, and SVC • VPLS/H-VPLS • MPLS TE, RSVP TE • Multicast VPN • 6PE, 6VPE
Availability	• VRRP/VRRP v3 • VRRP load balancing mode • MPLS TE FRR • IP FRR: static routing/policy-based routing/RIP/IS-IS/OSPF • IGP fast routing convergence • BFD: supporting collaboration with static route/RIP/OSPF/ISIS/BGP/VRRP/TE FRR/IPv6 • NQA: Network Quality Analysis, supporting collaboration with VRRP, policy routing, and static routing • GR: OSPF/BGP/IS-IS/LDP/RSVP • In-service hotfix • Hot swapping of interface modules, fan trays and power modules • ISSU
Management and maintenance	• Configuration at the CLI • Configuration through the console port • Telnet for configuration and remote maintenance through Ethernet port • SNMP v1/v2c/v3 • RMON (group 1, 2, 3 and 9 MIB) • System logs • Hierarchical alarms • Ping and Tracert • Fan status detection, maintenance, and alarming • Power supply status detection, maintenance, and alarming • CF card status detection and maintenance

	• Temperature detection and alarming • EAA
File system	• FAT format • CF card • Dual image
Uploading and upgrading	• Loading/upgrading through the Xmodem protocol • Loading/upgrading through File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP)

Appendix B Software upgrading

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

Startup software images

The router supports main startup images and backup startup images.

At startup, the router always attempts to boot first with the main startup image. If the attempt fails, for example, because the image file is corrupted, the router tries to boot with the backup startup images.

The startup images are saved in .bin files. The following table lists the default storage media for saving the files:

Device model	Default storage medium	Default access path
HSR6600	Flash memory	flash:/

The examples in this chapter use the flash memory as the storage medium.

Upgrade methods

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

Upgrade method	Remarks
Upgrading startup images from the CLI	You must reboot the router to complete the upgrade. This method can interrupt ongoing network services.
Upgrading startup images from the extended BootWare menu	Use this method when the router cannot correctly start up.
Upgrading BootWare from the extended BootWare menu	N/A

Preparing for software upgrade

Before you upgrade system software, complete the following tasks:

- Configure routes. Make sure 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 the upgrade has minimal impact on the network services. During the upgrade, the router cannot provide any services.

IMPORTANT:

To use the extended BootWare menu to download files through an Ethernet port, make sure the Ethernet port is M-GE0/0/0 on an HSR6600 router.

Upgrading startup images from the CLI

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

Using TFTP to upgrade startup images

This section describes how to upgrade system software by using TFTP.

Backing up the current configuration file and software image files

1. Save the current configuration.

```
<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.
<Sysname>
```

2. Identify the current configuration file and software image files. Verify that the flash memory has sufficient space for the upgrade file and the new software image files. If the space is not sufficient, use the **delete /unreserved** *file-url* command to permanently delete unused files, or use the **reset recycle-bin** command to release the space used by files in the recycle bin.

```
<Sysname> dir
Directory of flash:
   0 drw-           - Aug 12 2013 16:38:21   diagfile
   1 -rw-         895 Aug 20 2013 09:33:00   ifindex.dat
   2 drw-           - Aug 13 2013 09:51:02   logfile
   3 drw-           - Aug 12 2013 16:38:21   seclog
   4 -rw-     9427968 Aug 12 2013 16:34:56   HSR6602-cmw710-boot-r7103p01.bin
   5 -rw-   107847680 Aug 12 2013 16:35:23   HSR6602-cmw710-system-r7103p01.bin
   6 -rw-        3740 Aug 20 2013 09:33:01   startup.cfg
   7 -rw-      114861 Aug 20 2013 09:33:01   startup.mdb

524288 KB total (407549 KB free)

<Sysname>
```

3. Back up the configuration file **startup.cfg** to the TFTP server.

```
<Sysname> tftp 192.168.2.80 put startup.cfg
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 17683    0     0  100 17683      0   279k --:--:-- --:--:-- --:--:--  297k
<Sysname>
```

Upgrading the startup images

1. Download the upgrade file HSR6602.ipe to the flash memory on the router.

```
<Sysname> tftp 192.168.2.80 get HSR6602.ipe
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  111M    0  111M    0     0   314k      0 --:--:--  0:06:04 --:--:--  318k
<Sysname>
```

2. Specify the image files in the upgrade file as the main startup image files.

```
<Sysname> boot-loader file flash:/HSR6602.ipe slot 0 main
Verifying the IPE file and the images.............Done.
HPE HSR6602 images in IPE:
  HSR6602-CMW710-BOOT-R7103P08.bin
  HSR6602-CMW710-SYSTEM-R7103P08.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 0.
Decompressing file HSR6602-CMW710-BOOT-R7103P08.bin to
flash:/HSR6602-CMW710-BOOT-R7103P08.bin.......Done.
Decompressing file HSR6602-CMW710-SYSTEM-R7103P08.bin to
flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin.......................................
..............................Done.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software images for
all slots.
Do you want to delete flash:/HSR6602.ipe now? [Y/N]:y
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 0.
<Sysname>
```

3. Verify that the image files have been configured as main startup image files.

```
<Sysname> display boot-loader
Software images on slot 0:
Current software images:
  flash:/HSR6602-CMW710-BOOT-R7103P08.bin
  flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin
Main startup software images:
  flash:/HSR6602-CMW710-BOOT-R7103P08.bin
  flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin
Backup startup software images:
  None
```

4. Reboot the router to load the main startup image files.

```
<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...
%Aug 20 10:44:06:159 2015 HPE DEV/5/SYSTEM_REBOOT: System is rebooting now.

System is starting...
```

5. Verify that the router is using the correct image files.

```
<Sysname> display version
HPE Comware Software, Version 7.1.054, Release 7103P08
Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP
HPE HSR6602-XG uptime is 0 weeks, 0 days, 2 hours, 58 minutes
Last reboot reason : Exception reboot
Boot image: flash:/HSR6602-CMW710-BOOT-R7103P08.bin
Boot image version: 7.1.054, Release 7103P08
  Compiled Feb 23 2016 16:00:01
System image: flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin
System image version: 7.1.054, Release 7103P08
  Compiled Feb 23 2016 16:00:01

Slot 1/0: HSR6602-XG uptime is 0 week, 0 day, 2 hours, 58 minutes
 CPU type: FREESCALE P4080 1500MHz
 2048M bytes DDR3 SDRAM Memory
 8M bytes Flash Memory
 128K bytes NVRAM
 PCB              Version: Ver.A
 Basic      Logic Version: 1.0
 Extend     Logic Version: 2.0
 Basic   BootWare Version: 2.03
 Extend  BootWare Version: 2.03
 [FIXED PORTS] MGE             (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
 [FIXED PORTS] Combo 4GE       (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
 [FIXED PORTS] 2XGE            (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0

Slot 1/1: FIP-20 uptime is 0 week, 0 day, 2 hours, 58 minutes
 PCB              Version: Ver.A
 Logic            Version: 1.0
 Basic   BootWare Version: 0.00
 Extend  BootWare Version: 0.00
 [SUBSLOT   1] RT-HIM-16GBP     (Hardware)Ver.A,   (Driver)1.0,   (Cpld)133.0
 [SUBSLOT   2] 8GBE            (Hardware)Ver.B,   (Driver)1.0,   (Cpld)3.0

<Sysname>
```

Using FTP to upgrade startup images

This section describes how to upgrade system software by using FTP.

Backing up the current configuration file and software image files

1. Save the current configuration.

```
<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.
<Sysname>
```

2. Identify the current configuration file and software image files. Verify that the flash memory has sufficient space for the upgrade file and the new software image files. If the space is not sufficient, use the **delete /unreserved** *file-url* command to permanently delete unused files, or use the **reset recycle-bin** command to release the space used by files in the recycle bin.

```
<Sysname> dir
Directory of flash:
   0 drw-           - Aug 12 2013 16:38:21   diagfile
   1 -rw-         895 Aug 20 2013 09:33:00   ifindex.dat
   2 drw-           - Aug 13 2013 09:51:02   logfile
   3 drw-           - Aug 12 2013 16:38:21   seclog
   4 -rw-     9427968 Aug 12 2013 16:34:56   HSR6602-cmw710-boot-r7103p01.bin
   5 -rw-   107847680 Aug 12 2013 16:35:23   HSR6602-cmw710-system-r7103p01.bin
   6 -rw-        3740 Aug 20 2013 09:33:01   startup.cfg
   7 -rw-      114861 Aug 20 2013 09:33:01   startup.mdb

524288 KB total (407549 KB free)

<Sysname>
```

3. Connect to the FTP server.

```
<Sysname> ftp 192.168.2.80
Press CTRL+C to abort.
Connected to 192.168.2.80 (192.168.2.80).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.2.80:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
```

4. Back up the configuration file **startup.cfg** to the FTP server.

```
ftp> binary
200 Type is Image (Binary)
ftp> put startup.cfg
.227 Entering Passive Mode (192,168,2,80,12,101)
150 "C:\USERS\XXXXX\DESKTOP\SOFTWARE\startup.cfg" file ready to receive in IMAG
E / Binary mode
226 Transfer finished successfully.
3740 bytes sent in 0.000 seconds (9.15 Mbytes/s)
ftp>
```

Upgrading the startup images

1. Download the upgrade file **HSR6602.ipe** to the flash memory on the router.

```
ftp> get HSR6602.ipe
.227 Entering Passive Mode (192,168,2,80,12,111)
150 "C:\USERS\XXXXX\DESKTOP\SOFTWARE\HSR6602.ipe" file ready to send (117424128
 bytes) in IMAGE / Binary mode
................................................................................
.....
receive aborted
waiting for remote to finish abort
426 Transfer aborted.
226 Abort Successful.
116490240 bytes received in 85.680 seconds (1.30 Mbytes/s)
ftp>
```

2. Return to user view.

```
ftp> quit
221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye
<Sysname>
```

3. Specify the image files in the upgrade file as the main startup image file.

```
<Sysname> boot-loader file flash:/HSR6602.ipe slot 0 main
Verifying the IPE file and the images..............Done.
HPE HSR6602 images in IPE:
  HSR6602-CMW710-BOOT-R7103P08.bin
  HSR6602-CMW710-SYSTEM-R7103P08.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 0.
Decompressing file HSR6602-CMW710-BOOT-R7103P08.bin to flash:/HSR6602-CMW710-BOO
T-R7103P08.bin.......Done.
Decompressing file HSR6602-CMW710-SYSTEM-R7103P08.bin to flash:/HSR6602-CMW710-S
YSTEM-R7103P08.bin..............................................................
........Done.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software image
s for all slots.
Do you want to delete flash:/HSR6602.ipe now? [Y/N]:y
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 0.
<Sysname>
```

4. Verify that the image files have been configured as main startup image files.

```
<Sysname> display boot-loader
Software images on slot 0:
Current software images:
  flash:/HSR6602-CMW710-BOOT-R7103P08.bin
  flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin
Main startup software images:
  flash:/HSR6602-CMW710-BOOT-R7103P08.bin
  flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin
Backup startup software images:
  None
```

5. Reboot the router to load the main startup image files.

```
<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...
%Aug 20 10:44:06:159 2015 HPE DEV/5/SYSTEM_REBOOT: System is rebooting now.

System is starting...
```

6. Verify that the router is using the correct image files.

```
<Sysname> display version
HPE Comware Software, Version 7.1.054, Release 7103P08
Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP
HPE HSR6602-XG uptime is 0 weeks, 0 days, 2 hours, 58 minutes
Last reboot reason : Exception reboot
Boot image: flash:/HSR6602-CMW710-BOOT-R7103P08.bin
Boot image version: 7.1.054, Release 7103P08
  Compiled Feb 23 2016 16:00:01
System image: flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin
System image version: 7.1.054, Release 7103P08
  Compiled Feb 23 2016 16:00:01

Slot 1/0: HSR6602-XG uptime is 0 week, 0 day, 2 hours, 58 minutes
 CPU type: FREESCALE P4080 1500MHz
 2048M bytes DDR3 SDRAM Memory
 8M bytes Flash Memory
 128K bytes NVRAM
 PCB              Version: Ver.A
 Basic      Logic Version: 1.0
 Extend     Logic Version: 2.0
 Basic   BootWare Version: 2.03
 Extend  BootWare Version: 2.03
 [FIXED PORTS] MGE              (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
 [FIXED PORTS] Combo 4GE        (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0
 [FIXED PORTS] 2XGE             (Hardware)Ver.A,   (Driver)1.0,   (Cpld)2.0

Slot 1/1: FIP-20 uptime is 0 week, 0 day, 2 hours, 58 minutes
 PCB              Version: Ver.A
 Logic            Version: 1.0
 Basic   BootWare Version: 0.00
 Extend  BootWare Version: 0.00
 [SUBSLOT   1] RT-HIM-16GBP     (Hardware)Ver.A,   (Driver)1.0,   (Cpld)133.0
 [SUBSLOT   2] 8GBE             (Hardware)Ver.B,   (Driver)1.0,   (Cpld)3.0

<Sysname>
```

Upgrading startup images from the extended BootWare menu

You can use the following methods to upgrade startup images from the extended BootWare menu:

- Using TFTP/FTP to upgrade startup images through an Ethernet port
- Using Xmodem to upgrade startup images through the console port

TIP:

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

Accessing the extended BootWare menu

1. Power on the router. The following startup information appears:

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

****************************************************************************
*                                                                          *
*                      HPE Router BootWare, Version 2.03                   *
*                                                                          *
****************************************************************************
Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP

Compiled Date       : Nov  6 2015
CPU Type            : P4080
CPU L1 Cache        : 32KB
CPU Clock Speed     : 1500MHz
Memory Type         : DDR3 SDRAM
Memory Size         : 2048MB
Memory Speed        : 650MHz
BootWare Size       : 1024KB
Flash Size          : 8MB
Nand Flash size     : 512MB
NVRAM Size          : 128KB
BASIC CPLD Version  : 1.0
EXTENDED CPLD Version: 2.0
PCB Version         : Ver.A


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

2. Press **Ctrl** + **B** at the prompt. The extended BootWare menu appears.

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

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

Table 8 Extended BootWare menu options

Item	Description
<1> Boot System	Boot the system software image.
<2> Enter Serial SubMenu	Access the Serial submenu (see Table 11) for upgrading system software through the console port or changing the serial port settings.
<3> Enter Ethernet SubMenu	Access the Ethernet submenu (see Table 9) for upgrading system software through an Ethernet port or changing Ethernet settings.
<4> File Control	Access the File Control submenu (see Table 13) to retrieve and manage the files stored on the router.
<5> Restore to Factory Default Configuration	Restore the factory defaults. This option is not supported when the password recovery feature is enabled.
<6> Skip Current System Configuration	Start the router with the factory default configuration. This option is not supported when the password recovery feature is disabled.
<7> BootWare Operation Menu	Access the BootWare Operation menu for backing up, restoring, or upgrading BootWare. When you upgrade the system software image, BootWare is automatically upgraded. Hewlett Packard Enterprise recommends not upgrading BootWare separately.
<8> Skip Authentication for Console Login	Skip console login authentication. This option is not supported when the password recovery feature is disabled.
<9> Storage Device Operation	Access the Storage Device Operation menu to manage storage devices. Using this option is beyond this chapter.
<0> Reboot	Restart the router.

Using TFTP/FTP to upgrade startup images through an Ethernet port

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

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

Table 9 Ethernet submenu options

Item	Description
<1> Download Image Program To SDRAM And Run	Download a software image to the SDRAM and run the image. This option is not supported when the password recovery feature is disabled.
<2> Update Main Image File	Upgrade the main startup images. The newly loaded software image files are configured with the M attribute. The original main startup image files lose the M attribute.
<3> Update Backup Image File	Upgrade the backup startup images. The newly loaded startup image files are configured with the B attribute. The original backup startup image files lose the B attribute.
<4> Download Files(*.*)	Download files to the router. This option is not supported when the password recovery feature is disabled.
<5> Modify Ethernet Parameter	Modify network settings.
<0> Exit To Main Menu	Return to the extended BootWare menu.

2. Enter **5** to configure the network settings.

```
==========================<ETHERNET PARAMETER SET>==========================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|         Ctrl+D = Quit.                                                   |
============================================================================
Protocol (FTP or TFTP) :ftp
Load File Name         :HSR6602.ipe
                       :
Target File Name       :HSR6602.ipe
                       :
```

```
Server IP Address      :192.168.2.80
Local IP Address       :192.168.2.62
Subnet Mask            :0.0.0.0
Gateway IP Address     :0.0.0.0
FTP User Name          :test
FTP User Password      :***
```

Table 10 Network parameter fields and shortcut keys

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

3. Enter **2** or **3** in the Ethernet submenu to upgrade the main or backup startup images. For example, enter **2** to upgrade the main startup images.

```
Loading.....................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
.......................................................Done.
117424128 bytes downloaded!
Image file HSR6602-CMW710-BOOT-R7103P08.bin is self-decompressing...
Saving file flash:/HSR6602-CMW710-BOOT-R7103P08.bin ........................
........................Done.
Image file HSR6602-CMW710-SYSTEM-R7103P08.bin is self-decompressing...
Saving file flash:/HSR6602-CMW710-SYSTEM-R7103P08.bin ......................
```

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

4. Enter **0** to return to the extended BootWare menu or enter **1** to boot the system.

Using Xmodem to upgrade startup images through the console port

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

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

Table 11 Serial submenu options

Item	Description
<1> Download Image Program To SDRAM And Run	Download startup image files to the SDRAM and run the images. This option is not supported when the password recovery feature is disabled.
<2> Update Main Image File	Upgrade the main startup images. The newly loaded software image files are configured with the M attribute. The original main startup image files lose the M attribute.
<3> Update Backup Image File	Upgrade the backup system software image. The newly loaded startup image files are configured with the B attribute. The original

Item	Description
	backup startup image files lose the B attribute.
<4> Download Files(*.*)	Download files to the router. This option is not supported when the password recovery feature is disabled.
<5> Modify Serial Interface Parameter	Modify serial port parameters
<0> Exit To Main Menu	Return to the extended BootWare menu.

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

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

The following messages appear:

```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

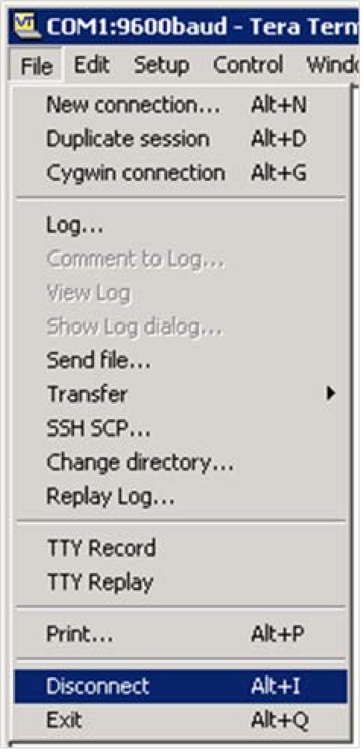
3. Change the baud rate of the HyperTerminal to be the same as the device's console port:

NOTE:

If you select the default baud rate (9600 bps), skip this step, and directly go to step 4.

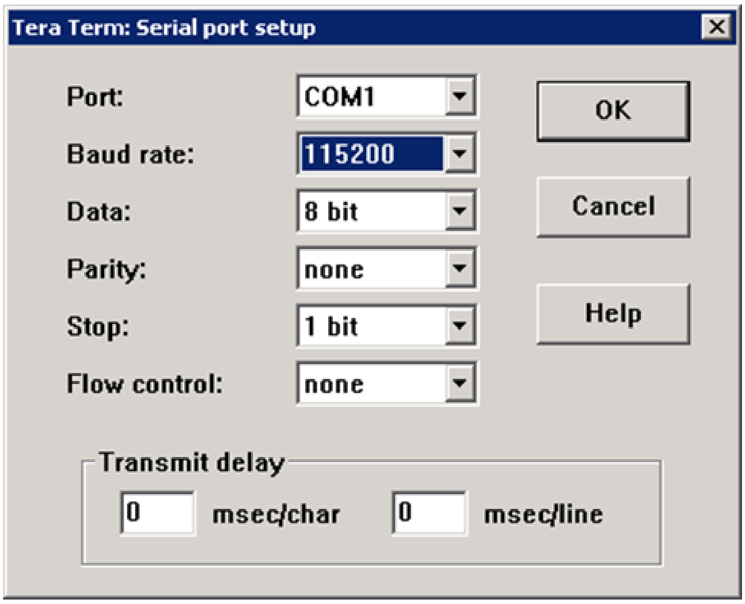
a. Select **File** > **Disconnect** from the menu bar of Tera Term.

Figure 1 File > Disconnect menu



b. Set the baud rate to 115200, and then click **OK**.

Figure 2 Serial port setup


Tera Term: Serial port setup

Port: COM1

Baud rate: 115200

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

Transmit delay

0 msec/char 0 msec/line

c. In the terminal display window, press **Enter** to reconnect to the device.

4. At the prompt for download confirmation, enter **y** to download software images.

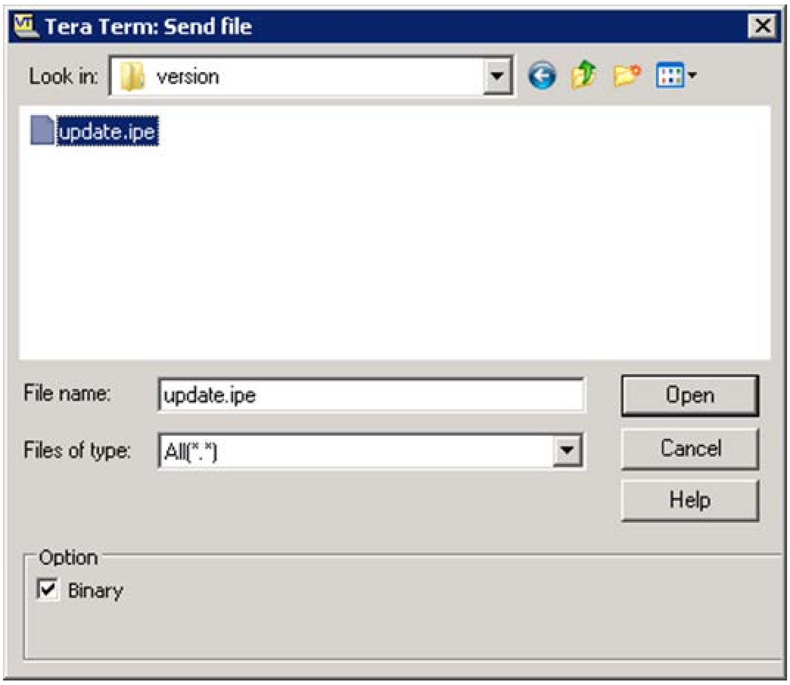
```
Are you sure to download file to flash? Yes or No (Y/N):Y
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCC
```

If you enter **n**, the system returns to the Serial submenu.

To abort the downloading task after you enter **y**, press **Ctrl**+**X**.

5. Select **File** > **Send File** from the menu bar of Tera Term.
6. In the file selection dialog box, select the upgrade image file and the **Binary** option.

Figure 3 Selecting the file to transfer



Look in: version

update.ipe

File name: update.ipe

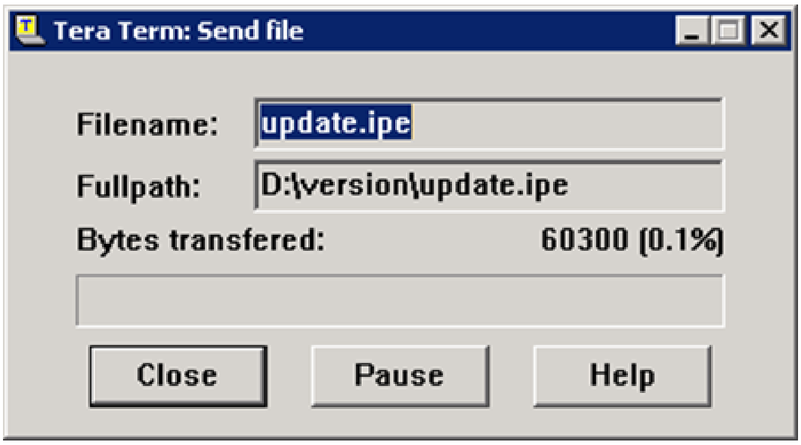
Files of type: All(*.*)

Option

☑ Binary

7. Click **Open**.

Figure 4 File transfer progress



Filename: update.ipe

Fullpath: D:\version\update.ipe

Bytes transfered: 60300 (0.1%)

8. At the prompt for image attribute, enter **m** to specify the file as the main (primary) startup image file.

NOTE:

- If you enter **b**, the image file attribute is set to **Backup**. The image file will be used only if the main image is not available or corrupt.
- If you enter **n**, the image file attributed is set to **None**. The image file will not be used for startup.

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
Load File name  : default_file boot-update.bin
Free space: 470519808 bytes
Writing flash...................................................................
.............Done!
The system-update.bin image is self-decompressing...
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:

If a file already exists with the same attribute as the upgrade file, the attribute of that file changes to **None**.

9. Change the baud rate of the terminal emulator back to 9600.

Skip this step if you have not changed the default baud rate of the terminal.

10. Press **Enter** to reconnect to the device.

11. In the extended BootWare menu menu, enter **0** to reboot the device. The device starts up with the downloaded image file.

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

Upgrading BootWare from the extended BootWare menu

Preparing for the upgrade

1. Connect the router to the PC where the upgrade file is stored through the management Ethernet port.
2. Connect the router to the same PC or a different PC through the console port.
3. Run a TFTP or FTP server on the PC connected through the management Ethernet port.
4. Correctly set the working directory on the TFTP or FTP server, and set the username and password for login.
5. Run a terminal emulation program on the PC connected through the console port.

Upgrade procedure

1. Enter the extended BootWare menu (see Accessing the extended BootWare menu), and enter **7** to access the BootWare Operation menu.

```
=========================<BootWare Operation Menu>==========================
|Note:the operating device is flash                                        |
|<1> Backup Full BootWare                                                  |
|<2> Restore Full BootWare                                                 |
|<3> Update BootWare By Serial                                             |
|<4> Update BootWare By Ethernet                                           |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

2. Enter **4** to access the BootWare Operation Ethernet submenu.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extended BootWare                                              |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

3. Enter **4** to configure the network settings.

```
==========================<ETHERNET PARAMETER SET>==========================
|Note:       '.' = Clear field.                                            |
|            '-' = Go to previous field.                                   |
|         Ctrl+D = Quit.                                                   |
============================================================================
Protocol (FTP or TFTP) :ftp
Load File Name         :HSR6602.btw
                       :
Target File Name       :HSR6602.btw
                       :
Server IP Address      :192.168.2.80
```

```
Local IP Address       :192.168.2.62
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
FTP User Name          :abc
FTP User Password      :***
```

NOTE:

Enter a new value directly for a parameter, or use the default value for a parameter by pressing **Enter**.

Table 12 Network parameter fields and shortcut keys

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

After you configure network settings, the following submenu appears:

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extend BootWare                                                |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

4. Enter a number in the range of 1 to 3. For example, enter **1** to upgrade the entire BootWare.

```
Loading...........Done!
447612 bytes downloaded!
Updating Basic BootWare? [Y/N]
```

5. Enter **y** to upgrade the basic segment of BootWare.

```
Updating Basic BootWare.........Done!
Updating Extend BootWare? [Y/N]
```

6. Enter **y** to upgrade the extended segment of BootWare.

```
Updating Extend BootWare.........Done!

===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extend BootWare                                                |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

7. Enter **0** in the BootWare Operation Ethernet submenu to return to the BootWare Operation menu.
8. Enter **0** in the BootWare Operation menu to return to the extended BootWare menu.
9. Enter **0** in the extended BootWare menu to reboot the router.

Managing files from the extended BootWare menu

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

The File Control submenu appears:

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

Table 13 File Control submenu options

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

Displaying all files

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

```
Display all file(s) in flash:
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                           |
|1   114861    Aug/20/2015 09:33:01 N/A    flash:/startup.mdb             |
|2   3740      Aug/20/2015 09:33:01 M      flash:/startup.cfg             |
|3   895       Aug/20/2015 09:33:00 N/A    flash:/ifindex.dat             |
|4   42544     Aug/13/2015 09:51:02 N/A    flash:/logfile/logfile1.log    |
|5   107847680 Aug/20/2015 17:10:11 M      flash:/HSR6602-cmw710-system-r71|
|03p06.bin                                                                |
|6   9427968   Aug/20/2015 17:09:47 M      flash:/HSR6602-cmw710-boot-r7103|
|p06.bin                                                                  |
|7   116494336 Aug/20/2015 10:56:11 N/A    flash:/HSR6602.ipe             |
|8   0         Aug/20/2015 09:16:15 N/A    flash:/.trash/.trashinfo       |
============================================================================
```

Changing the type of a startup image file

Startup image file attributes include main (M) and backup (B). You can specify neither, either, or both of the attributes for an image file. If you do not specify an attribute, the file attribute is marked as **N/A**. If you specify both of the attributes, the file attribute is marked as **M+B**.

Two boot image files or system image files on the same MPU cannot have the same attribute. For example, if a boot image file with the **M+B** attribute exists, no other boot image file with the **M** or **B** attribute can exist. If you change the attribute of a second boot image file to **M** or **B**, the **M+B** attribute of the first file changes to **B** or **M**.

To change the type of a startup image file:

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

```
'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                           |
|1   116494336 Aug/20/2015 10:56:11 N/A    flash:/HSR6602.ipe             |
|0   Exit                                                                 |
============================================================================
Enter file No.:
```

2. Enter the number of the startup image file and press **Enter**.

```
Modify the file attribute:
============================================================================
|<1>+Main                                                                 |
|<2>+Backup                                                               |
|<0> Exit                                                                 |
============================================================================
Enter your choice(0-2):
```

3. Enter **1** or **2** to add a file attribute for the file.

```
This operation may take several minutes. Please wait....
Image file HSR6602.ipe is self-decompressing...
```

```
Saving file
flash:/HSR6602.ipe ........................................................
.................Done.
Set the file attribute success!
```

Deleting files

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

To delete files:

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

```
Deleting the file in flash:
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                            |
|1   114861    Aug/20/2015 09:33:01 N/A    flash:/startup.mdb              |
|2   3740      Aug/20/2015 09:33:01 M      flash:/startup.cfg              |
|3   895       Aug/20/2015 09:33:00 N/A    flash:/ifindex.dat              |
|4   42544     Aug/13/2015 09:51:02 N/A    flash:/logfile/logfile1.log     |
|5   107847680 Aug/20/2015 17:10:11 M      flash:/HSR6602-cmw710-system-r71|
|03p06.bin                                                                 |
|6   9427968   Aug/20/2015 17:09:47 M      flash:/HSR6602-cmw710-boot-r7103|
|p06.bin                                                                   |
|7   116494336 Aug/20/2015 10:56:11 N/A    flash:/HSR6602.ipe              |
|8   0         Aug/20/2015 09:16:15 N/A    flash:/.trash/.trashinfo        |
============================================================================
Enter file No.:
```

2. Enter the number of the file to be deleted. For example, enter **2** to delete the **startup.cfg** file.

```
The file you selected is flash:/startup.cfg,Delete it? [Y/N]
```

3. Enter **y**.

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

Handling software upgrade failures

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

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

7. Verify that the startup image version matches the BootWare version. For compatibility information about startup image versions and BootWare versions, see the release notes for the router.

Hewlett Packard
Enterprise

HPE HSR6602-CMW710-R7103P09 Release Notes

Software Feature Changes

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

Contents

R7103P09

This release has the following changes:

- Configuring the MIM-1CT3 interface module
- Modified feature: Support for WAN interface commands in CT3 interface view
- Modified feature: Displaying track entry information

New feature: Configuring the MIM-1CT3 interface module

Configuring the MIM-1CT3 interface module

Both T3 and T1 belong to the T-carrier system promoted by ANSI. T3 uses the digital signal level DS-3 and operates at 44.736 Mbps.

CT3 interfaces support T3 (unchannelized) mode and CT3 (channelized) mode.

- In T3 mode, a CT3 interface provides 44.736 Mbps of data bandwidth. No timeslots are divided. The system automatically creates a synchronous serial interface for it. The serial interface name uses the **serial** *number***/0:0** format.
- In CT3 mode, a CT3 interface can be demultiplexed into 28 channels of T1 signals. Each T1 line can be divided into 24 timeslots numbered 1 through 24. Each line on a T1 interface can operate at either 64 kbps or 56 kbps.

  The following are schemes available for creating different rates of T1 lines on a CT3 interface in CT3 mode:

  - *M* × 1.536 Mbps. (*M* is an integer in the range of 1 to 28.)
  - *N* × 56 kbps or N x 64 kbps. (*N* is an integer in the range of 1 to 300.)

  A T1 line can operate in T1 or CT1 mode.

  - If the T1 line operates in unframed (T1) mode, the system automatically creates a 1544 kbps serial interface for it. The serial interface name uses the **serial** *number***/***line-number***:0** format.
  - If the T1 line operates in framed (CT1) mode, you can bundle timeslots on it. The system automatically creates a synchronous serial interface for it. The serial interface name uses the **serial** *number***/***line-number***:***set-number* format. This interface operates at *n* × 64 kbps or *n* × 56 kbps, where *n* is the number of bundled timeslots.
- The synchronous serial interface created in T3 or CT3 mode has the same logical features as a standard synchronous serial interface and supports the following protocols:
  - Data link layer protocols, such as PPP, HDLC, and Frame Relay.
  - Network layer protocols, such as IP.

  You can configure this interface in the same way you configure a standard synchronous serial interface.

Configuring a CT3 interface in T3 mode

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter CT3 interface view.	**controller t3** *interface-number*	N/A
3. Configure the interface to operate in T3 mode.	**using t3**	The default operating mode is

Step	Command	Remarks
		CT3 mode.
4. (Optional.) Configure the interface to operate in the FT3 mode and set the DSU mode or the subrate.	**ft3** { **dsu-mode** { **0** | **1** | **2** | **3** | **4** } | **subrate** *number* }	By default, DSU mode 0 (the digital link mode) is used, and the subrate is 44210 kbps.
5. (Optional.) Configure the interface description.	**description** *text*	By default, the description of an interface is *interface-name* **Interface**.
6. Set the clock mode.	**clock** { **master** | **slave** }	The default clock mode for the CT3 interface is **slave**, which is line clock.
7. Set the cable length.	**cable** *feet*	The default is 14.9 meters (49 feet).
8. (Optional.) Set the loopback mode.	**loopback** { **local** | **payload** | **remote** }	By default, loopback is disabled.
9. (Optional.) Configure alarm signal detection/sending.	**alarm** { **detect** | **generate** { **ais** | **febe** | **idle** | **rai** } }	By default, alarm signal detection is enabled and alarm signal sending is disabled.
10. (Optional.) Configure FEAC channel signal detection/sending on the CT3 interface.	• **feac detect** • **feac generate loopback** { **ds3-line** | **ds3-payload** } • **feac generate** { **ds3-los** | **ds3-ais** | **ds3-oof** | **ds3-idle** | **ds3-eqptfail** }	By default, FEAC channel signal detection is enabled, but no FEAC signals are sent.
11. (Optional.) Configure MDL message detection/sending on the CT3 interface.	**mdl** { **data** { **eic** *string* | **fic** *string* | | **gen-no** *string* | **lic** *string* | **pfi** *string* | **port-no** *string* | **unit** *string* } | **detect** | **generate** { **idle-signal** | **path** | **test-signal** } }	By default, MDL message detection and sending are disabled and the default MDL message information applies.
12. (Optional.) Restore the default settings for the CT3 interface.	**default**	N/A
13. (Optional.) Bring up the CT3 interface.	**undo shutdown**	By default, a CT3 interface is up.
14. Return to system view.	**quit**	N/A
15. Enter synchronous serial interface view.	**interface serial** *number***/0:0**	Make sure the synchronous serial interface is the one created for the CT3 interface.
16. Set the CRC mode.	**crc** { **16** | **32** | **none** }	The default is 16-bit CRC.

Configuring a CT3 interface in CT3 mode

When you change the interface state during the configuration, make sure you understand the following information:

- Shutting down or bringing up a CT3 interface also shuts down or brings up all its lines and serial interfaces, including:
    - T1 lines demultiplexed from the CT3 interface.
    - Serial interfaces created for unframed T1 lines.
    - Serial interfaces created for channel sets on framed T1 lines.

- Shutting down or bringing up a T1 line also shuts down or brings up the serial interface created for it.
- To shut down or bring up only the serial interface for a T3, unframed T1, or framed T1 channel, use the **shutdown** or **undo shutdown** command in serial interface view.

To configure a CT3 interface in CE3 mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter CT3 interface view.	**controller t3** *interface-number*	N/A
3. Configure the interface to operate in CT3 mode.	**using ct3**	The default operating mode is CT3 mode.
4. Set the operating mode of a T1 line on the CT3 interface.	• Set the operating mode to unframed (T1): **t1** *line-number* **unframed** • Set the operating mode to framed (CT1) and bundle timeslots: **a.** (Optional.) **undo t1** *line-number* **unframed** **b.** **t1** *line-number* **channel-set** *set-number* **timeslot-list** *range* [**speed** { **56k** | **64k** }]	By default: • A T1 line operates in framed (CT1) mode. • No channel sets exist on a T1 line.
5. (Optional.) Configure the interface description.	**description** *text*	By default, the description of an interface is *interface-name* **Interface**.

6. (Optional.) Set the clock mode.	• Set the clock mode for a CT3 interface:
	clock { **master** | **slave** }
	• Set the clock mode for a T1 line on the CT3 interface:
	t1 *line-number* **clock** { **master | slave** }
		The default clock mode for the CT3 interface is **slave**.
		The default clock mode for the T1 line is **slave**.

7. Set the cable length.	**cable** *feet*	The default is 14.9 meters (49 feet).
8. Set the framing format for the CT3 interface.	**frame-format** { **c-bit** | **m23** }	By default, the framing format on the CT3 interface is C-bit.
9. Set the framing format for the T1 line.	**t1** *line-number* **frame-format** { **esf | sf** }	By default, the framing format on the T1 line is ESF.

10. (Optional.) Set the loopback mode.	• On the CT3 interface:
	loopback { **local** | **payload** | **remote** }
	• On a T1 line:
	t1 *line-number* **loopback** { **local** | **payload** | **remote** }
		By default, loopback is disabled.

11. (Optional.) Configure alarm signal detection/sending.	• On the CT3 interface:
	alarm { **detect** | **generate** { **ais** | **febe** | **idle** | **rai** } }
	• On a T1 line:
	t1 *line-number* **alarm** { **detect | generate** { **ais** | **rai** } }
		By default, alarm signal detection is enabled and alarm signal sending is disabled.

12. (Optional.) Configure FEAC channel signal	• **feac detect**	By default, FEAC channel signal detection is enabled, but no FEAC

Step	Command	Remarks
detection/sending on the CT3 interface.	- **feac generate loopback** { **ds3-line** | **ds3-payload** } - **feac generate** { **ds3-los** | **ds3-ais** | **ds3-oof** | **ds3-idle** | **ds3-eqptfail** }	signals are sent.
13. (Optional.) Configure MDL message detection/sending on the CT3 interface.	**mdl** { **data** { **eic** *string* | **fic** *string* | | **gen-no** *string* | **lic** *string* | **pfi** *string* | **port-no** *string* | **unit** *string* } | **detect** | **generate** { **idle-signal** | **path** | **test-signal** } }	By default, MDL message detection and sending are disabled and the default MDL message information applies.
14. (Optional.) Place a T1 line on the far-end CT3 interface in a loopback.	**t1** *line-number* **sendloopcode** { **fdl-ansi-line-up** | **fdl-ansi-payload-up** | **fdl-att-payload-up** | **inband-line-up** }	By default, no loopback mode is set.
15. (Optional.) Set the FDL format for a T1 channel.	**t1** *line-number* **set fdl** { **ansi** | **att** | **both** | **none** }	By default, FDL is disabled. This operation applies only to T1 channels that are formed on CT3 interfaces, operate in channelized mode, and use ESF as the T1 framing format.
16. (Optional.) Restore the default settings for the CT3 interface.	**default**	N/A
17. (Optional.) Bring up the CT3 interface or a T1 line on the interface.	- Bring up the CT3 interface: **undo shutdown** - Bring up a T1 line on the CT3 interface: **undo t1** *line-number* **shutdown**	By default, all CT3 interfaces and T1 lines are up.
18. Return to system view.	**quit**	N/A
19. Enter synchronous serial interface view.	- In T1 mode: **interface serial** *number***/***line-number***:0** - In CT1 mode: **interface serial** *number/line-number***:***set-number*	Make sure the synchronous serial interface is the one created for the T1 line you want to configure.
20. Set the CRC mode.	**crc** { **16** | **32** | **none** }	The default is 16-bit CRC.

Displaying and maintaining CT3 interfaces

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

Task	Command
Display CT3 interface information.	**display controller t3** [*interface-number*]
Display the configuration and state of a serial interface formed on a CT3 interface.	**display interface serial** *interface-number*
Display the state of a T1 line.	**t1** *line-number* **show**
Clear statistics for CT3 interfaces.	**reset counters controller t3** [*interface-number*]

Command reference

alarm

Use **alarm** to enable a CT3 interface to detect/send alarm signals.

Use **undo alarm** to remove the alarm signal detection/sending setting.

Syntax

alarm { **detect** | **generate** { **ais** | **febe** | **idle** | **rai** } }

undo alarm { **detect** | **generate** { **ais** | **febe** | **idle** | **rai** } }

Default

Periodic alarm detection is enabled.

Default

Alarm signal sending is disabled.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

detect: Enables periodical alarm signal detection.

generate: Sends alarm signals for line state test.

- **ais**: Alarm indication signal.
- **febe**: Far end block error signal.
- **idle**: Idle signal.
- **rai**: Remote alarm indication signal.

Usage guidelines

At startup, periodical alarm signal detection is enabled on the CT3 interface. When the interface detects LOS, LOF, or AIS signals, it sends RAI signals to its peer.

The supported alarm signals (LOS, LOF, AIS, RAI, FEBE, and idle) are ANSI T1.107-1995 compliant.

You can configure the CT3 interface to send a type of alarm signal. To send another type of signal, you must first remove the previous setting by using the **undo alarm** command. If a RAI signal is present because an LOS, LOF, or AIS alarm is detected, you must first use the **undo alarm detect** command to remove the signal.

To display the real-time alarm state on the CT3 interface, use the **display controller t3** command.

Examples

# Enable periodical alarm signal detection on CT3 interface T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] alarm detect
```

# Enable CT3 interface T3 2/4/0 to send AIS alarm signals.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] alarm generate ais
```

cable

Use **cable** to configure the cable length on a CT3 interface.

Use **undo cable** to restore the default.

Syntax

cable *feet*

undo cable

Default

The cable length on a CT3 interface is 49 feet (14.9 meters).

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

feet: Cable length in the range of 0 to 450 feet (0 to 137.2 meters).

Usage guidelines

The cable length in this command refers to the distance between the router and the cable distribution rack.

Examples

# Set the cable length to 50 feet (15.24 meters) on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] cable 50
```

clock

Use **clock** to set the clock mode of a CT3 interface.

Use **undo clock** to restore the default.

Syntax

clock { **master | slave** }

undo clock

Default

The clock mode for a CT3 interface is **slave**.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

master: Sets the clock mode to **master**.

slave: Sets the clock mode to **slave**.

Usage guidelines

When the clock mode of a CT3 interface is **master**, it uses the internal clock source. When the clock mode of a CT3 interface is **slave**, it uses the line clock source.

When connected to a transmission device, the CT3 interface must use the **slave** clock. The clock provided by the transmission device is more precise.

When two CT3 interfaces are directly connected, you must configure the two ends with different clock modes.

Examples

# Set the clock mode to **master** for T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] clock master
```

controller t3

Use **controller t3** to enter CT3 interface view.

Syntax

controller t3 *interface-number*

Views

System view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a CT3 interface by its number.

Examples

# Enter the view of T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0]
```

display controller t3

Use **display controller t3** to display information about CT3 interfaces.

Syntax

display controller t3 [*interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-number: Specifies a CT3 interface by its number. If you do not specify this argument, the command displays information about all CT3 interfaces.

Usage guidelines

In addition to the state information about the CT3 interface, the command displays information about each T1 line on the CT3 interface if the interface is operating in CT3 mode.

Examples

# Display information about T3 2/4/0.

```
<Sysname> display controller t3 2/4/0
T3 2/4/0
Current state: UP
Description: T3 2/4/0 Interface
Basic Configuration:
  Work mode is CT3, cable length is 49 feet
  Frame-format is C-BIT Parity, line code is B3ZS
  Source clock is slave, loopback is not set
Alarm state:
  Receiver alarm state is none
MDL state:
  No message is sent now.
  Message data elements:
    EIC: line, LIC: line, FIC: line, UNIT: line
    FI: line, PORT_NO: line
    GEN_NO: line
  Periodical detection is disabled
FEAC state:
  No code is sent now. DS3 LOS(because of receive Alarm) was last sent.
  Periodical detection is enabled, no code received now.
 DS3 Out-of-Frame last received.
BERT state:(stopped)
Historical Statistics:
  Data in current interval (22 seconds elapsed):
    1 Line Code Violations, 0 Far End Block Error
0 C-Bit Coding Violation, 1 P-bit Coding Violation
0 ulFraming Bit Err, 0 Severely Err ulFraming Secs
0 C-bit Err Secs, 0 C-bit Severely Err Secs
1 P-bit Err Secs, 0 P-bit Severely Err Secs
56 Unavailable Secs, 1 Line Err Secs

 T3 2/4/0  CT1 1 is up
   Frame-format ESF, clock slave, loopback not set
   FDL Performance Report is disabled
   Receiver alarm state is none
   BERT state:(stopped)
```

Table 1 Command output

Field	Description
Current state	Physical link state of the interface: • **Administratively DOWN**—The interface has been shut down by using the **shutdown** command. • **DOWN**—The interface is administratively up, but its physical state is down (possibly because no physical link exists or the link has failed). • **UP**—The interface is both administratively and physically up.
Description	Description of the interface.
Basic Configuration	Basic configurations of the interface.
Work mode	Operating mode of the interface: CT3 or T3.
cable length	Cable length supported by the interface.
Frame-format	Frame format: C-bit parity or M23.
Source clock	Clock source used by the interface: master or slave.
loopback	Loopback setting on the interface: local, remote, payload, or not set.
Receiver alarm state is none	Type of the received alarm: none, LOS, LOF, RAI, or AIS. If the interface receives a LOS, LOF, or AIS alarm and sends out an RAI alarm, **Transmitter is sending RAI** is displayed.
No message is sent now.	No MDL message is being sent. If an MDL message, path or idle-signal for example, is being sent, **Message sent now: path. idle signal** is displayed.
Message data elements	MDL data elements.
EIC: line, LIC: line, FIC: line, UNIT: line	EIC, LIC, FIC, and UNIT are four elements present in all types of MDL messages. Their values are user configurable and default to line.
FI: line, PORT_NO: line	FI is contained in MDL path messages and PORT_NO is contained in MDL idle signal messages. Their values are user configurable and default to line.
GEN_NO: line	GEN_NO is contained in MDL test signal messages. Its value is user configurable and defaults to line.
Periodical detection	State of periodical detection of MDL. Periodical MDL message detection is disabled by default at the startup of the router. When this function is enabled, **Periodical detection is enabled** is displayed. When MDL messages are detected, information about detected MDL messages is displayed.
No code is sent now. DS3 LOS(because of receive Alarm) was last sent.	No FEAC signal is sent. The FEAC signal sent last time is DS3 Loss-of-Signal.
Periodical detection is enabled, no code received now.	Periodical detection of FEAC is enabled and no FEAC signal is received now. Periodical FEAC signal detection is enabled by default at the startup of the router.
DS3 Out-of-Frame last received	The FEAC signal received last time is DS3 Out-of-Frame.
BERT state:(stopped)	BERT state. BERT is not supported in the current software version.

Field	Description
Data in current interval (22 seconds elapsed):	Statistics spanning the current 15-minute interval.
Line Code Violations	Line code violations: BPV, or EXZ.
Far End Block Error	Far-end block error.
C-Bit Coding violation	C-bit coding violation.
P-bit Coding Violation	P-bit coding violation.
ulFraming Bit Err	Framing bit error.
Severely Err ulFraming Secs	Severely erroneous second.
C-bit Err Secs	C-bit erroneous second.
C-bit Severely Err Secs	C-bit severely erroneous second.
P-bit Err Secs	P-bit erroneous second.
P-bit Severely Err Secs	P-bit severely erroneous second.
Unavailable Secs	Service unavailable second.
Line Err Secs	Line erroneous second, during which LOS, BPV, EXZ, C-bit, P-bit, and other errors occur.
Data in Interval 1:	Statistics spanning interval 1.
Total Data (last 17 15 minute intervals)	Total data spanning the last 17 intervals.
T3 2/4/0 CT1 1 is up	State of T1 line on the CT3 interface: up or down. In this output sample, T1 line 1 is up.
Frame-format ESF, clock slave, loopback not set	Information about the T1 line: • **Framing format**—ESF or SF. • **Clock source**—Slave for the line clock and master for the internal clock. • **Loopback**—Local, remote, payload, or not set.
FDL Performance Report is disabled	Transmission of PPR in the FDL is disabled. You can enable it by using the **t1 fdl** command.
Transmitter is sending RAI	The transmitter of the T1 line is sending RAI signals. When the T1 line receives LOS, LOF, or AIS signals, it sends RAI signals.
Receiver alarm state	Type of alarm signal that the T1 line can receive: LOS, LOF, AIS, or RAI.
Line loop back activate code using inband signal last sent	The loopback code sent last time is in-band LLB activation request code.

Related commands

reset counters controller t3

feac

Use **feac** to enable far end and control signal (FEAC) channel signal detection and transmission on a CT3 interface.

Use **undo feac** to remove the current FEAC settings.

Syntax

feac { **detect** | **generate** { **ds3-los** | **ds3-ais** | **ds3-oof** | **ds3-idle** | **ds3-eqptfail** | **loopback** { **ds3-line** | **ds3-payload** } } }

undo feac { **detect** | **generate** { **ds3-los** | **ds3-ais** | **ds3-oof** | **ds3-idle** | **ds3-eqptfail** | **loopback** { **ds3-line** | **ds3-payload** } } }

Default

On a CT3 interface, periodical FEAC channel signal detection is enabled, and FEAC signal transmission is disabled.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

detect: Enables periodical FEAC channel signal detection.

generate: Generates a specific type of FEAC signal.

- **ds3-los**: Specifies the DS3 LOS signal.
- **ds3-ais**: Specifies the DS3 AIS signal.
- **ds3-oof**: Specifies the DS3 OOF signal.
- **ds3-idle**: Specifies the DS3 idle signal.
- **ds3-eqptfail**: Specifies DS3 equipment failure signal.

loopback: Sends a specific type of loopback code for activating a specific loopback.

- **ds3-line**: Specifies far-end line loopback.
- **ds3-payload**: Specifies payload loopback.

Usage guidelines

FEAC is a channel formed by using the third C-bit in the first subframe in C-bit framing. The channel is used for the following purposes:

- Transmits alarm state signals for line test.
- Transmits loopback control code to activate or deactivate far-end loopback during a loopback test.

According to ANSI T1.107a, the framing format of FEAC channels is bit-oriented protocol (BOP).

After far-end loopback is activated by using the **feac generate loopback** { **ds3-line** | **ds3-payload** } command, you can remove it by using the **undo** form of the command.

Before you configure far-end loopback by using this command, disable FEAC detection on the local end to prevent loopback deadlock. Loopback deadlock occurs when the local end enables loopback after detecting the loopback code sent back by the far end.

To display the transmitting and receiving state of the FEAC channel, use the **display controller t3** command.

Examples

# Enable FEAC channel signal detection on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] feac detect
```

# Send DS3 LOS signal on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] feac generate ds3-los
```

# On T3 2/4/0, send loopback code to the far end to place the far end in a line loopback.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] feac generate loopback ds3-line
```

frame-format

Use **frame-format** to set the framing format for a CT3 interface.

Use **undo frame-format** to restore the default.

Syntax

frame-format { **c-bit** | **m23** }

undo frame-format

Default

The framing format for a CT3 interface is C-bit.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

c-bit: Sets the framing format to C-bit.

m23: Sets the framing format to m23.

Usage guidelines

This command is available only in channelized mode.

Examples

# Set the framing format to **m23** for T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] frame-format m23
```

Related commands

using

ft3

Use **ft3** to configure a CT3 interface to operate in FT3 mode and set the DSU mode or the subrate.

Use **undo ft3** to restore the default.

Syntax

ft3 { **dsu-mode** { **0** | **1** | **2** | **3** | **4** } | **subrate** *number* }

undo ft3 { **dsu-mode** | **subrate** }

Default

DSU mode 0 (the Digital Link mode) is used, and the subrate is 44210 kbps.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

dsu-mode: Specifies the DSU mode.

Table 2 FT3 DSU mode options

Keyword	DSU mode (vendor)	Subrate range	Total number of subrate grades
0	Digital Link	300 to 44210 kbps in steps of 300746 bps	147
1	Kentrox	1500 to 35000 kbps in steps of 500000 bps 44210 kbps	69
2	Larscom	3100 to 44210 kbps in steps of 3157835 bps	14
3	Adtran	75 to 44210 kbps in steps of 75187 bps	588
4	Verilink	1500 to 44210 kbps in steps of 1578918 bps	20

subrate *number*: Specifies the subrate for the CT3 interface. The *number* argument is in the range of 1 to 44210 (in kbps).

Usage guidelines

This command is available only in T3 mode.

FT3 (Fractional T3 or Subrate T3) mode is a nonstandard E3 application mode. FE3 subrate ranges and the number of subrate grades vary by vendor. You can use the **ft3** command to configure the device to be compatible with the FE3 DSU modes listed in Table 16.

After you set the subrate by using the **ft3 subrate** command, the T3 interface searches the subrate levels corresponding to the DSU mode in which it is operating. The T3 interface selects the subrate level that is closest to subrate level set by the **ft3 subrate** command. The device adjusts the hardware to allow for the subrate.

You can use the **display interface serial** *interface-number***:0** command to check the DSU mode setting, the subrate, the actual rate, and the baud rate of a CT3 interface. The actual rate does not count in the overhead bits. The baud rate is the actual T3 line rate (44736 kbps), with the overhead bits counted in.

Examples

# Configure T3 2/4/0 to operate in the FT3 mode. Set the DSU mode to 1 and the subrate to 3000 kbps.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] using t3
[Sysname-T3 2/4/0] ft3 dsu-mode 1
[Sysname-T3 2/4/0] ft3 subrate 3000
```

loopback

Use **loopback** to enable a type of loopback on a CT3 interface.

Use **undo loopback** to disable loopback on a CT3 interface.

Syntax

loopback { **local** | **payload** | **remote** }

undo loopback

Default

Loopback is disabled on CT3 interfaces.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

local: Enables internal loopback.

payload: Enables external payload loopback.

remote: Enables external loopback.

Usage guidelines

Loopback is intended for testing only. Disable the feature when the interface is operating correctly.

If a CT3 interface encapsulated with PPP is placed in a loopback, the state of the link layer protocol is reported as down.

Examples

# Enable internal loopback on interface T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] loopback local
```

mdl

Use **mdl** to configure MDL message detection and transmission on a CT3 interface.

Use **undo mdl** to restore the default.

Syntax

mdl { **data** { **eic** *string* **|** **fic** *string* **|** **gen-no** *string* **|** **lic** *string* **|** **pfi** *string* **|** **port-no** *string* **|** **unit** *string* } **|** **detect** **|** **generate** { **idle-signal** **|** **path** **|** **test-signal** } }

undo mdl [**data** [**eic** **|** **fic** **|** **gen-no** **|** **lic** **|** **pfi** **|** **port-no** **|** **unit**] **|** **detect** **|** **generate** [**idle-signal** **|** **path** **|** **test-signal**]]

Default

Periodic MDL detection is disabled. CT3 interfaces do not send MDL messages.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

data: Sets MDL message parameters. If you do not specify a parameter, a default string of **line** is set in the MDL messages.

- **eic** *string*: Specifies the equipment identification code, a string of 1 to 10 characters. This parameter is contained in all three types of MDL messages.
- **fic** *string*: Specifies the frame identification code, a string of 1 to 10 characters. This parameter is contained in all three types of MDL messages.
- **gen-no** *string*: Specifies the generator number, a string of 1 to 38 characters. This parameter is specific to test signal messages.
- **lic** *string*: Specifies the location identification code, a string of 1 to 11 characters. This parameter is contained in all three types of MDL messages.
- **pfi** *string*: Specifies the path facility identification, a string of 1 to 38 characters. This parameter is specific to path messages.
- **port-no** *string*: Specifies the port number in idle signal message, a string of 1 to 38 characters. This parameter is specific to idle signal messages.
- **unit** *string*: Specifies the unit, a string of 1 to 6 characters. This parameter is contained in all three types of MDL messages.

detect: Enables periodical MDL message detection.

generate: Sends a specific type of MDL message.

- **idle-signal**: Specifies MDL idle signal messages.
- **path**: Specifies MDL path messages.
- **test-signal**: Specifies MDL test signal messages.

Usage guidelines

MDL is a channel formed by using the three C-bits in the fifth subframe in C-bit framing. According to ANSI T1.107a, MDL can transmit path, idle signal, and test signal messages. The data framing format is LAPD for MDL messages.

To send idle signal, path, and test signal messages simultaneously, repeat the **mdl** command to specify the **idle-signal**, **path**, and **test-signal** keywords.

To display the receiving and transmission status of the MDL link, use the **display controller t3** command.

Examples

# Enable MDL detection on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] mdl detect
```

# Set LIC to **hello** for CT3 interface T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] mdl data lic hello
```

# Send path messages on CT3 interface T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] mdl generate path
```

reset counters controller t3

Use **reset counters controller t3** to clear CT3 interface statistics.

Syntax

reset counters controller t3 [*interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface-number: Specifies a CT3 interface by its number. If you do not specify this argument, the command clears statistics for all CT3 interfaces.

Usage guidelines

To display CT3 interface statistics, use the **display controller t3** command.

Examples

# Clear statistics for T3 2/4/0.

```
<Sysname> reset counters controller t3 2/4/0
```

Related commands

display controller t3

t1 alarm

Use **t1 alarm** to enable a T1 line on a CT3 interface to detect/send alarm signals.

Use **undo t1 alarm** to remove the alarm signal detection/sending setting.

Syntax

t1 *line-number* **alarm** { **detect** | **generate** { **ais** | **rai** } }

undo t1 *line-number* **alarm** { **detect** | **generate** { **ais** | **rai** } }

Default

On a CT3 interface, periodical alarm detection is enabled, and alarm signal sending is disabled.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

detect: Specifies periodical alarm signal detection.

generate: Sends a specific type of alarm signals. These alarm signals are used for line status test.

- **ais**: Alarm indication signal.
- **rai**: Remote alarm indication signal.

Usage guidelines

At startup, periodical alarm signal detection is enabled on all T1 lines on the CT3 interface. When a T1 line detects LOS, LOF, or AIS signals, it sends RAI signals to its peer.

The supported alarm signals (LOS, LOF, AIS, RAI, FEBE, and idle) are ANSI T1.403 compliant.

Only one type of alarm signal can be sent on a T1 line at a time. To send another type of signal, you must first remove the previous setting by using the **undo t1 alarm** command. If a RAI signal is present because an LOS, LOF, or AIS alarm is detected, you must first use the **undo t1 alarm detect** command to remove the signal.

To display the real-time alarm state on T1 lines, use the **display controller t3** command.

Examples

# Enable periodical alarm signal detection on T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 alarm detect
```

# Enable T1 line 1 on T3 2/4/0 to send AIS alarm signals.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 alarm generate ais
```

t1 channel-set

Use **t1 channel-set** to bundle timeslots into a channel set on a T1 line.

Use **undo t1 channel-set** to remove a channel set.

Syntax

t1 *line-number* **channel-set** *set-number* **timeslot-list** *list* [**speed** { **56k** | **64k** }]

undo t1 line-number **channel-set** set-number

Default

No channel sets exist on a T1 line.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

set-number: Specifies the number of a channel set created by timeslot bundling on a T1 line, in the range of 0 to 23.

timeslot-list *list*: Specifies a comma-separated list of timeslot items. An item can be an individual timeslot or a timeslot range. Use a hyphen (-) to separate the start and end timeslot numbers of a range. The value range for the timeslot number is 1 to 24.

speed { **56k** | **64k** }: Speed of the timeslot bundle (the channel set) in kbps. If **56k** is selected, the timeslots are bundled into an *n* × 56 kbps bundle. If **64k**, the default, is selected, the timeslots are bundled into an *n* × 64 kbps bundle.

Usage guidelines

When a T1 line is operating in framed (CT1) mode, you can bundle timeslots on it. For each channel set, the system automatically creates a serial interface named **serial** *number***/***line-number***:***set-number*. This interface operates at *n* × 64 kbps or *n* × 56 kbps, where *n* is the number of bundled timeslots. This interface has the same logical features as a standard synchronous serial interface. You can configure this serial interface in the same way you configure a standard synchronous serial interface.

Examples

# Create a 128 kbps serial interface through timeslot bundling on T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 channel-set 1 timeslot-list 1,2
```

Related commands

t1 unframed

t1 clock

Use **t1 clock** to set the clock mode of a T1 line on a CT3 interface.

Use **undo t1 clock** to restore the default.

Syntax

t1 *line-number* **clock** { **master** | **slave** }

undo t1 *line-number* **clock**

Default

The clock mode of a T1 line on a CT3 interface is **slave**.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

master: Sets the clock mode to **master**.

slave: Sets the clock mode to **slave**.

Usage guidelines

When the clock mode of a T1 line is **master**, it uses the internal clock source. When the clock mode of a T1 line is **slave**, it uses the line clock source.

When a CT3 interface is operating in channelized mode, its T1 lines might use separate clocks.

Examples

# Set the clock mode to **slave** for T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 clock slave
```

t1 fdl

Use **t1 fdl** to set the behavior of a T1 line on the FDL in ESF framing.

Use **undo t1 fdl** to disable FDL of T1.

Syntax

t1 *line-number* **fdl** { **ansi** | **att** | **both** | **none**}

undo t1 line-number **fdl**

Default

FDL is disabled in ESF framing.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

ansi: Specifies ANSI T1.403 for FDL.

att: Specifies AT&T TR 54016 for FDL.

both: Specifies both ANSI T1.403 and AT&T TR 54016 for FDL.

none: Disables the use of FDL on the T1 line.

Usage guidelines

FDL is an embedded 4 kbps overhead channel within the ESF format for transmitting periodical performance report (PPR) statistics or loopback code.

According to ANSI T1.403, the format of PPR is LAPD, and the format of loopback code is BOP.

The **t1 set fdl** command only starts PPR transmission. It cannot enable loopback code transmission or detection.

This command only applies to channelized T1 lines with a T1 frame format of ESF.

Examples

# Set the FDL to be ANSI T1.403 compliant for T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 fdl ansi
```

Related commands

t1 frame-format

t1 frame-format

Use **t1 frame-format** to set the framing format for a T1 line.

Use **undo t1 frame-format** to restore the default.

Syntax

t1 *line-number* **frame-format** { **esf** | **sf** }

undo t1 *line-number* **frame-format**

Default

The framing format of a T1 line is ESF.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

esf: Sets the T1 line to use the ESF format.

sf: Sets the T1 line to use the SF format.

Usage guidelines

You can configure this command only when the T1 line is operating in framed mode. To configure a T1 line to operate in framed mode, use the **undo t1 unframed** command.

Examples

# Set the framing format to SF for T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 frame-format sf
```

Related commands

t1 unframed

t1 loopback

Use **t1 loopback** to enable a type of loopback for a T1 line on a CT3 interface.

Use **undo t1 loopback** to disable loopback for a T1 line on a CT3 interface.

Syntax

t1 *line-number* **loopback** { **local** | **payload** | **remote** }

undo t1 *line-number* **loopback**

Default

Loopback is disabled on T1 lines.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

local: Enables internal loopback.

payload: Enables payload loopback mode.

remote: Enables external loopback.

Usage guidelines

Loopback is intended for testing only. Disable the feature when the interface is operating correctly.

If a T1 line encapsulated with PPP is in loopback mode, the state of the link layer protocol is reported as down.

Examples

# Enable internal loopback on T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 loopback local
```

t1 sendloopcode

Use **t1 sendloopcode** to set the loopback mode of a far-end T1 line.

Use **undo t1 sendloopcode** to remove the corresponding setting.

Syntax

t1 *line-number* **sendloopcode** { **fdl-ansi-line-up** | **fdl-ansi-payload-up** | **fdl-att-payload-up** | **inband-line-up** }

undo t1 *line-number* **sendloopcode** { **fdl-ansi-line-up** | **fdl-ansi-payload-up** | **fdl-att-payload-up** | **inband-line-up** }

Default

No loopback mode is set.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number, in the range of 1 to 28.

fdl-ansi-line-up: Sends ANSI-compliant LLB activation request code in the FDL to start remote loopback.

fdl-ansi-payload-up: Sends ANSI-compliant PLB activation request code in the FDL to start remote loopback.

fdl-att-payload-up: Sends AT&T-compliant PLB activation request code in the FDL to start remote loopback.

inband-line-up: Sends in-band LLB activation request code compliant with the ANSI and AT&T implementation to start remote loopback.

Usage guidelines

Loopback is an effective method of diagnosis. You can place a far-end device into loopback mode either at the command line on it or by sending loopback control code to it. The types and formats of loopback control code supported on T1 interfaces are compliant with ANSI T1.403.

Loopback can be divided into line loopback and payload loopback. The data stream is looped back at the framer only in the line loopback.

You can transmit loopback control code by using the in-band signal (the 192 effective bandwidth bits or all 193 bits of T1) or the FDL in ESF frames.

Examples

# Send the in-band signal on T1 line 1 on T3 2/4/0 to place the far-end T1 line in line loopback mode.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 sendloopcode inband-line-up
```

t1 show

Use **t1 show** to have a quick look at the line state of a T1 line on a CT3 interface.

Syntax

t1 line-number **show**

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

show: Displays the physical line state of the specified T1 line.

Examples

# Display line state of T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 show
T3 2/4/0  CT1 1: up
  Frame-format ESF, clock slave, loopback not set
  FDL Performance Report is disabled
  Receiver alarm state is none
  BERT state:(stopped)
```

Table 3 Command output

Field	Description
T3 2/4/0 CT1 1 is up	State of T1 line 1 on the CT3 interface: up or down.
Frame-format	Framing format of T1: ESF or SF.
clock	Clock source used by the T1 line: slave for the line clock or master for the internal clock.
loopback	Loopback state or mode: local, remote, payload, or not set.
FDL Performance Report is disabled	Transmission of PPR in the FDL is disabled. You can enable it by using the **t1 fdl ansi** command.
Transmitter is sending RAI	The transmitter of the T1 line is sending RAI signals. When the T1 line receives LOS, LOF, or AIS signals, it sends RAI signals.
Receiver alarm state	Type of alarm signal that the T1 line can receive: LOS, LOF, AIS, or RAI.
Line loop back activate code using inband signal last sent	The loopback code sent last time is in-band LLB activation request code.
BERT state	BERT state. BERT is not supported in the current software version.

t1 shutdown

Use **t1 shutdown** to shut down a T1 line on a CT3 interface.

Use **undo t1 shutdown** to bring up a T1 line.

Syntax

t1 *line-number* **shutdown**

undo t1 *line-number* **shutdown**

Default

T1 lines on a CT3 interface are up.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

Usage guidelines

Shutting down or bringing up a T1 line also shuts down or brings up the serial interface created for it.

Examples

# Shut down T1 line 1 on T3 2/4/0.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 shutdown
```

t1 unframed

Use **t1 unframed** to set a T1 line on a CT3 interface to operate in unframed mode (T1 mode).

Use **undo t1 unframed** to set a T1 line on a CT3 interface to operate in framed mode (CT1 mode).

Syntax

t1 *line-number* **unframed**

undo t1 *line-number* **unframed**

Default

T1 lines on a CT3 interface are operating in framed mode.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

line-number: Specifies a T1 line number in the range of 1 to 28.

Usage guidelines

A T1 line in unframed mode does not contain frame control information or support timeslot division. The system automatically creates a 1544 kbps serial interface named **serial** *number***/***line-number***:0**. This interface has the same logical features as a standard synchronous serial interface. You can configure this serial interface in the same way you configure a standard synchronous serial interface.

Examples

# Set T1 line 1 on T3 2/4/0 to operate in unframed mode.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] t1 1 unframed
```

Related commands

t1 channel-set

using

Use **using** to configure the operating mode of a CT3 interface.

Use **undo using** to restore the default.

Syntax

using { **ct3** | **t3** }

undo using

Default

A CT3 interface operates in channelized mode.

Views

CT3 interface view

Predefined user roles

network-admin

Parameters

ct3: Sets the CT3 interface to operate in channelized mode.

t3: Sets the CT3 interface to operate in unchannelized mode.

Usage guidelines

You can only configure T1 lines on CT3 interfaces in channelized mode.

When a CT3 interface operates in unchannelized mode, the system automatically creates a 44.736 Mbps serial interface named **serial** *number***/0:0** for it. This interface has the same logical features as a standard synchronous serial interface. You can configure this serial interface in the same way you configure a standard synchronous serial interface.

Examples

# Configure T3 2/4/0 to operate in unchannelized mode.

```
<Sysname> system-view
[Sysname] controller t3 2/4/0
[Sysname-T3 2/4/0] using t3
```

Modified feature: Support for WAN interface commands in CT3 interface view

Feature change description

The following WAN interface commands became available in CT3 interface view:

- **default**
- **description**
- **shutdown**

Command changes

None

Modified feature: Displaying track entry information

Feature change description

You can display track entries in Negative or Positive state and display brief track entry information.

Command changes

Modified command: display track

Old syntax

display track { *track-entry-number* **|** **all** }

New syntax

display track { *track-entry-number* **|** **all** [**negative** **|** **positive**] } [**brief**]

Views

Any view

Change description

The following keywords were added to the **display track** command:

- **negative**: Displays track entries in Negative state.
- **positive**: Displays track entries in Positive state.
- **brief**: Displays brief information about track entries.

R7103P08

This release has the following changes:

New feature: Initial down event timeout timer for BFD sessions

Setting the initial down event timeout timer for BFD sessions

This feature enables BFD to notify the upper-layer protocol of the events for failure to establish control packet mode BFD sessions. The upper-layer protocol can take correct actions based on the notification.

Command reference

bfd init-fail timer

Use **bfd init-fail-timer** to set the initial down event timeout timer for BFD sessions.

Use **undo bfd init-fail-timer** to restore the default.

Syntax

bfd init-fail-timer *seconds*

undo bfd init-fail-timer

Default

BFD does not notify the upper-layer protocol of the events for failure to establish control packet mode BFD sessions.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the initial down event timeout timer in the range of 5 to 600 seconds. BFD notifies the upper-layer protocol of initial down events after the timer expires.

Usage guidelines

Using this command can help the upper-layer protocol take correct actions. Take the link aggregation environment as an example. When the BFD session cannot come up because of link problems, the Ethernet link aggregation module cannot change the member port state from Selected to Unselected in time. To resolve this issue, you can use the **bfd init-fail-timer** command.

This command might cause the upper-layer protocol to take incorrect actions if the BFD session establishment failure is caused by configuration errors. Use it with caution.

This command does not take effect on echo packet mode BFD sessions.

Examples

# Set the initial down event timeout timer to 10 seconds for control packet mode BFD sessions.

```
<Sysname> system-view
[Sysname] bfd init-fail-timer 10
```

R7103P07

This release has the following changes:

Modified feature: Software image information display

Modified feature: Software image information display

Feature change description

The **Software image signature** field was added to the output from the following commands to display software image signature information:

- **display install active**
- **display install backup**
- **display install committed**
- **display install inactive**
- **display install ipe-info**
- **display install package**
- **display install which**

Values for the **Software image signature** field include:

- **HP**—For software images of the HP version.
- **HP-US**—For software images of the HP US version.
- **HPE**—For software images of the HP US version that have the HPE signature.

Command changes

None

R7103P06

This release has the following changes:

- New feature: Disabling alarm traps for transceiver modules
- New feature: Object group
- New feature: Maximum number of retransmission attempts for control packets
- Modified feature: Maximum value for the Layer 3 aggregate interface number
- Modified feature: Support for inter-AS IPv6 VPN option B
- Modified feature: Advertising the COMMUNITY attribute to a peer or peer group in BGP VPNv6 address family view or BGP-VPN IPv6 unicast address family view
- Modified feature: Configuring manual route summarization in BGP-VPN IPv6 unicast address family view
- Modified feature: Setting the OSPF SPF calculation interval
- Modified command: spf-schedule-interval
- Modified feature: Setting the LSU transmission interval

New feature: Disabling alarm traps for transceiver modules

Disabling alarm traps for transceiver modules

Disable alarm traps if the transceiver modules were manufactured or sold by Hewlett Packard Enterprise.

The device regularly detects transceiver modules that have a vendor name other than Hewlett Packard Enterprise or do not have a vendor name. Upon detecting such a transceiver module, the device repeatedly outputs traps and logs to notify the user to replace the module.

To disable alarm traps for transceiver modules:

Step	Command	Remarks
21. Enter system view.	**system-view**	N/A
22. Disable alarm traps for transceiver modules.	**transceiver phony-alarm-disable**	By default, alarm traps are enabled for transceiver modules.

Command reference

transceiver phony-alarm-disable

Use **transceiver phony-alarm-disable** to disable alarm traps for transceiver modules.

Use **undo transceiver phony-alarm-disable** to restore the default.

Syntax

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Default

Alarm traps are enabled for transceiver modules.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Disable alarm traps if the transceiver modules were manufactured or sold by Hewlett Packard Enterprise.

The device regularly detects transceiver modules that have a vendor name other than Hewlett Packard Enterprise or do not have a vendor name. Upon detecting such a transceiver module, the device repeatedly outputs traps and logs to notify the user to replace the module.

Examples

# Disable alarm traps for transceiver modules.

```
<Sysname> system-view
[Sysname] transceiver phony-alarm-disable
```

New feature: Object group

Overview

An object group is a group of objects that can be used by an ACL or object group to identify packets. Object groups are divided into the following types:

- **IPv4 address object group**—A group of IPv4 address objects used to match the IPv4 address in a packet.
- **IPv6 address object group**—A group of IPv6 address objects used to match the IPv6 address in a packet.
- **Port object group**—A group of port objects used to match the protocol port number in a packet.
- **Service object group**—A group of service objects used to match the upper-layer service in a packet.

Configuring an IPv4 address object group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure an IPv4 address object group and enter its view.	**object-group ip address** *object-group-name*	The system has one default IPv4 address object group.
3. (Optional.) Configure a description for the IPv4 address object group.	**description** *text*	By default, an object group does not have a description.
4. Configure an IPv4 address object.	[*object-id*] **network** { **host** { **address** *ip-address* | **name** *host-name* } | **subnet** *ip-address* { *mask-length* | *mask* } | **range** *ip-address1 ip-address2* |	By default, no objects exist.

Step	Command	Remarks
	group-object *object-group-name* }	

Configuring an IPv6 address object group

Step	Command	Remarks
5. Enter system view.	**system-view**	N/A
6. Configure an IPv6 address object group and enter its view.	**object-group ipv6 address** *object-group-name*	The system has one default IPv6 address object group.
7. (Optional.) Configure a description for the IPv6 address object group.	**description** *text*	By default, an object group does not have a description.
8. Configure an IPv6 address object.	[*object-id*] **network** { **host** { **address** *ipv6-address* | **name** *host-name* } | **subnet** *ipv6-address prefix-length* | **range** *ipv6-address1 ipv6-address2* | **group-object** *object-group-name* }	By default, no objects exist.

Configuring a port object group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a port object group and enter its view.	**object-group port** *object-group-name*	The system has one default port object group.
3. (Optional.) Configure a description for the port object group.	**description** *text*	By default, an object group does not have a description.
4. Configure a port object.	[*object-id*] **port** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* | **group-object** *object-group-name* }	By default, no objects exist.

Configuring a service object group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a service object group and enter its view.	**object-group service** *object-group-name*	The system has one default service object group.
3. (Optional.) Configure a description for the service object group.	**description** *text*	By default, an object group does not have a description.
4. Configure a service object.	[*object-id*] **service** { *protocol* [{ **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1*	By default, no objects exist.

Step	Command	Remarks
	port2 } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*] | **group-object** *object-group-name* }	

Displaying and maintaining object groups

Execute **display** commands in any view.

Task	Command
Display information about object groups.	**display object-group** [{ { **ip** | **ipv6** } **address** | **service** | **port** } [**default**] [**name** *object-group-name*] | **name** *object-group-name*]

Command reference

description

Use **description** to configure a description for an object group.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

No description is configured for an object group.

Views

Object group view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 127 characters.

Examples

# Configure the description as **This is an IPv4 object-group** for an IPv4 object group.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] description This is an IPv4 object-group
```

display object-group

Use **display object-group** to display information about object groups.

Syntax

display object-group [{ { **ip** | **ipv6** } **address** | **service** | **port** } [**default**] [**name** *object-group-name*] | **name** *object-group-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ip address: Specifies the IPv4 address object groups.

ipv6 address: Specifies the IPv6 address object groups.

port: Specifies the port object groups.

service: Specifies the service object groups.

default: Specifies the default object group.

name *object-group-name*: Specifies an object group by its name, a case-insensitive string of 1 to 31 characters.

Examples

# Display information about all object groups.

```
<Sysname> display object-group
IP address object group obj1: 0 object(in use)

IP address object group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1

IPv6 address object-group obj3: 0 object(in use)

IPv6 address object-group obj4: 5 objects(out of use)
0 network host address 1::1:1
10 network host name host
20 network subnet 1::1:0 112
30 network range 1::1:1 1::1:2
40 network group-object obj3

Service object-group obj5: 0 object(in use)

Service object-group obj6: 6 objects(out of use)
0 service 200
10 service tcp source lt 50 destination range 30 40
20 service udp source range 30 40 destination gt 30
30 service icmp 20 20
40 service icmpv6 20 20
50 service group-object obj5

Port object-group obj7: 0 object(in use)
Port object-group obj8: 3 objects(out of use)
0 port lt 20
10 port range 20 30
20 port group-object obj7
```

# Display information about object group **obj2**.

```
<Sysname> display object-group name obj2
IP address object-group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
```

# Display information about all IPv4 address object groups.

```
<Sysname> display object-group ip address
IP address object-group obj1: 0 object(in use)

IP address object-group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
```

# Display information about IPv6 address object group **obj4**.

```
<Sysname> display object-group ipv6 address name obj4
IPv6 address object-group obj4: 5 objects(out of use)
0 network host address 1::1:1
10 network host name host
20 network subnet 1::1:0 112
30 network range 1::1:1 1::1:2
40 network group-object obj3
```

Table 1 Command output

Field	Description
in use	The object group is used by an ACL or object group.
out of use	The object group is not used.

network (IPv4 address object group view)

Use **network** to configure an IPv4 address object.

Use **undo network** to delete an IPv4 address object.

Syntax

[*object-id*] **network** { **host** { **address** *ip-address* | **name** *host-name* } | **subnet** *ip-address* { *mask-length* | *mask* } | **range** *ip-address1 ip-address2* | **group-object** *object-group-name* }

undo network { **host** { **address** *ip-address* | **name** *host-name* } | **subnet** *ip-address* { *mask-length* | *mask* } | **range** *ip-address1 ip-address2* | **group-object** *object-group-name* }

undo *object-id*

Default

No IPv4 address objects exist.

Views

IPv4 address object group view

Predefined user roles

network-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not specify an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

host: Configures an IPv4 address object with the host address or name.

address *ip-address*: Specifies an IPv4 host address.

name *host-name*: Specifies a host name, a case-insensitive string of 1 to 60 characters.

subnet *ip-address* { *mask-length* | *mask* }: Configures an IPv4 address object with the subnet address followed by a mask length in the range of 0 to 32 or a mask in dotted decimal notation.

range *ip-address1 ip-address2*: Configures an IPv4 address object with the address range.

group-object *object-group-name*: Specifies an IPv4 address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command fails if you use it to configure or change an IPv4 address object to be identical with an existing object.

This command creates an IPv4 address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

If you configure a subnet with the mask length of 32 or the mask of 255.255.255.255, the system configures the object with a host address.

When you use the **range** *ip-address1 ip-address2* option, follow these guidelines:

- If *ip-address1* is equal to *ip-address2,* the system configures the object with a host address.
- If *ip-address1* is not equal to *ip-address2*, the system compares the two IPv4 addresses, configures a range starting with the lower IPv4 address, and performs the following operations:
    - Configures the object with an address range if the two addresses are in different subnets.
    - Configures the object with a subnet address if the two addresses are in the same subnet.

When you use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be an IPv4 address object group.
- If the specified object group does not exist, the system creates an IPv4 address object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

# Configure an IPv4 address object with the host address of **192.168.0.1**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] network host address 192.168.0.1
```

# Configure an IPv4 address object with the host name of **pc3**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network host name pc3
```

# Configure an IPv4 address object with the IPv4 address of **192.167.0.0** and mask length of **24**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.167.0.0 24
```

# Configure an IPv4 address object with the IPv4 address of **192.166.0.0** and mask of **255.255.0.0**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.166.0.0 255.255.0.0
```

# Configure an IPv4 address object with the address range of **192.165.0.100** to **192.165.0.200**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network range 192.165.0.100 192.165.0.200
```

# Configure an IPv4 address object using object group **ipgroup2**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network group-object ipgroup2
```

network (IPv6 address object group view)

Use **network** to configure an IPv6 address object.

Use **undo network** to delete an IPv6 address object.

Syntax

[*object-id*] **network** { **host** { **address** *ipv6-address* **|** **name** *host-name* } **|** **subnet** *ipv6-address prefix-length* **|** **range** *ipv6-address1 ipv6-address2* **|** **group-object** *object-group-name* }

undo network { **host** { **address** *ipv6-address* **|** **name** *host-name* } **|** **subnet** *ipv6-address prefix-length* **|** **range** *ipv6-address1 ipv6-address2* **|** **group-object** *object-group-name* }

undo *object-id*

Default

No IPv6 address objects exist.

Views

IPv6 address object group view

Predefined user roles

network-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not configure an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

host: Configures an IPv6 address object with the host address or name.

address *ipv6-address*: Specifies an IPv6 host address.

name *host-name*: Specifies a host name, a case-insensitive string of 1 to 60 characters.

subnet *ipv6-address prefix-length*: Configures an IPv6 address object with the subnet address followed by the prefix length in the range of 1 to 128.

range *ipv6-address1 ipv6-address2*: Configures an IPv6 address object.

group-object *object-group-name*: Specifies an IPv6 address object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command fails if you use it to configure or change an IPv6 address object to be identical with an existing object.

This command creates an IPv6 address object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

If you configure a subnet address with the prefix length of 128, the system configures the object with a host address.

When you use the **range** *ipv6-address1 ipv6-address2* option, follow these guidelines:

- If *ipv6-address1* is equal to *ipv6-address2,* the system configures the object with a host address.
- If *ipv6-address1* is not equal to *ipv6-address2*, the system compares the two IPv6 addresses, configures a range starting with the lower IPv6 address, and performs the following operations:
    - Configures the object with an address range if the two addresses are in different subnets.
    - Configures the object with a subnet address if the two addresses are in the same subnet.

When you use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be an IPv6 address object group.
- If the specified object group does not exist, the system creates an IPv6 address object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

# Configure an IPv6 address object with the host address of **1::1**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host address 1::1
```

# Configure an IPv6 address object with the host name of **pc3**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host name pc3
```

# Configure an IPv6 address object with the IPv6 address of **1:1:1::1** and prefix length of **24**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ip v6group] network subnet 1:1:1::1 24
```

# Configure an IPv6 address object with the address range of **1:1:1::1** to **1:1:1::100**

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network range 1:1:1::1 1:1:1::100
```

# Configure an IPv6 address object using object group **ipv6group2**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network group-object ipv6group2
```

object-group

Use **object-group** to configure an object group and enter its view, or enter the view of an existing object group.

Use **undo object-group** to delete an object group.

Syntax

object-group { { **ip** | **ipv6** } **address** | **port** | **service** } *object-group-name*

undo object-group { { **ip** | **ipv6** } **address** | **port** | **service** } *object-group-name*

Default

Each type of object group has a default object group named **any**.

Views

System view

Predefined user roles

network-admin

Parameters

ip address: Configures an IPv4 address object group.

ipv6 address: Configures an IPv6 address object group.

port: Configures a port object group.

service: Configures a service object group.

object-group-name: Specifies an object group name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

The **object-group** command execution results vary with the specified object group.

- If the specified group does not exist, the system creates a new object group and enters the object group view.
- If the specified group exists but the group type is different from that in the command, the command fails.

The **undo object-group** command execution results vary with the specified object group.

- If the specified group does not exist, the system executes the command without any system prompt.
- If the specified group exists and the group type is the same as that in the command, the system deletes the group.
- If the specified group exists but the group type is different from that in the command, the command fails.
- If the specified object group is being used by an ACL, object policy, or object group, the command fails.

The default object group cannot be deleted.

Examples

# Configure an IPv4 address object group named **ipgroup**.

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
```

# Configure an IPv6 address object group named **ipv6group**.

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
```

# Configure a port object group named **portgroup**.

```
<Sysname> system-view
[Sysname] object-group port portgroup
```

# Configure a service object group named **servicegroup**.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
```

port (port object group view)

Use **port** to configure a port object.

Use **undo port** to delete a port object.

Syntax

[*object-id*] **port** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* | **group-object** *object-group-name* }

undo port { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* | **group-object** *object-group-name* }

undo *object-id*

Default

No port objects exist.

Views

Port object group view

Predefined user roles

network-admin

Parameters

object-id: Specifies an object ID in the range of 0 to 4294967294. If you do not specify an object ID, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the system automatically assigns 30.

eq: Configures a port object with a port number equal to the specified port.

lt: Configures a port object with a port number smaller than the specified port.

gt: Configures a port object with a port number greater than the specified port.

port: Specifies a port number in the range of 0 to 65535.

range *port1 port2*: Configures a port object with a port range. The value range for the *port1* and *port2* arguments is 0 to 65535.

group-object *object-group-name*: Specifies a port object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command fails if you use it to configure or change a port object to be identical with an existing object.

This command creates a port object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

When you use the **lt** *port* option, follow these guidelines:

- The value of *port* cannot be 0.
- If the value of *port* is 1, the system configures the object with a port number of 0.
- If the value of *port* is in the range of 2 to 65535, the system configures the object with a port number range of [0, *port*–1].

When you use the **gt** *port* option, follow these guidelines:

- The value of *port* cannot be 65535.
- If the value of *port* is 65534, the system configures the object with a port number of 65535.
- If the value of *port* is in the range of 0 to 65533, the system configures the object with a port number range of [*port*+1, 65535].

When you use the **range** *port1 port2* option, follow these guidelines:

- If *port1* is equal to *port2*, the system configures the object with the port number *port1*.
- If *port1* is smaller than *port2*, the system configures the object with the port number range.
- If *port1* is greater than *port2*, the system changes the range to [*port2*, *port1*] and configures the object with the changed port number range.
- If *port1* is 0, the range is displayed as **lt** *port2*+1.
- If *port2* is 65535, the range is displayed as **gt** *port1*–1.

When you use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be a port object group.
- If the specified object group does not exist, the system creates a port object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

# Configure a port object with a port number of **100**.

```
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port eq 100
```

# Configure a port object with a port number smaller than **20**.

```
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port lt 20
```

# Configure a port object with a port number greater than **60000**.

```
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port gt 60000
```

# Configure a port object with a port number in the range of **1000** to **2000**.

```
<Sysname> system-view
[Sysname] object-group port portgroup
[Sysname-obj-grp-port-portgroup] port range 1000 2000
```

# Configure a port object using object group **portgroup2**.

```
<Sysname> system-view
[Sysname] object-group port portgroup
```

```
[Sysname-obj-grp-port-portgroup] port group-object portgroup2
```

service (service object group view)

Use **service** to configure a service object.

Use **undo service** to delete a service object.

Syntax

[*object-id*] **service** { *protocol* [{ **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*] | **group-object** *object-group-name* }

undo service { *protocol* [{ **source** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } | **destination** { { **eq** | **lt** | **gt** } *port* | **range** *port1 port2* } } * | *icmp-type icmp-code* | *icmpv6-type icmpv6-code*] | **group-object** *object-group-name* }

undo *object-id*

Default

No service objects exist.

Views

Service object group view

Predefined user roles

network-admin

Parameters

object-id: Configures an object ID in the range of 0 to 4294967294. If you do not configure an ID for the object, the system automatically assigns the object a multiple of 10 next to the greatest ID being used. For example, if the greatest ID is 22, the automatically assigned ID is 30.

protocol: Configures the protocol number in the range of 0 to 255, or the protocol name such as TCP, UDP, ICMP, and ICMPv6.

source: Configures a service object with a source port when the protocol is TCP or UDP.

destination: Configures a service object with a destination port when the protocol is TCP or UDP.

eq: Configures a port equal to the specified port.

lt: Configures a port smaller than the specified port.

gt: Configures a port greater than the specified port.

port: Specifies a port number in the range of 0 to 65535.

range *port1 port2*: Configures a service object with a port range. The value range for the *port1* and *port2* arguments is 0 to 65535.

icmp-type: Configures the ICMP message type in the range of 0 to 255.

icmp-code: Configures the ICMP message code in the range of 0 to 255.

icmpv6-type: Configures the ICMPv6 message type in the range of 0 to 255.

icmpv6-code: Configures the ICMPv6 message code in the range of 0 to 255.

group-object *object-group-name*: Specifies a service object group by its name, a case-insensitive string of 1 to 31 characters.

Usage guidelines

This command fails if you use it to configure or change a service object to be identical with an existing object.

This command creates a service object if the specified object ID does not exist. Otherwise, the command overwrites the configuration of the specified object.

When you use the **lt** *port* option, follow these guidelines:

- The value of *port* cannot be 0.
- If the value of *port* is 1, the system configures the object with a port number of 0.
- If the value of *port* is in the range of 2 to 65535, the system configures the object with a port number range of [0, *port*–1].

When you use the **gt** *port* option, follow these guidelines:

- The value of *port* cannot be 65535.
- If the value of *port* is 65534, the system configures the object with a port number of 65535.
- If the value of *port* is in the range of 0 to 65533, the system configures the object with a port number range of [*port*+1, 65535].

When you use the **range** *port1 port2* option, follow these guidelines:

- If *port1* is equal to *port2*, the system configures the object with the port number *port1*.
- If *port1* is smaller than *port2*, the system configures the object with the port number range.
- If *port1* is greater than *port2*, the system changes the range to [*port2*, *port1*] and configures the object with the changed port number range.
- If *port1* is 0, the range is displayed as **lt** *port2*+1.
- If *port2* is 65535, the range is displayed as **gt** *port1*–1.

When use the **group-object** *object-group-name* option, follow these guidelines:

- The object group to be used must be a service object group.
- If the specified object group does not exist, the system creates a service object group with the name you specified and uses the object group for the object.
- Two object groups cannot use each other at the same time.
- The system supports a maximum of five object group hierarchy layers. For example, if groups 1, 2, 3, and 4 use groups 2, 3, 4, and 5, respectively, group 5 cannot use another group and group 1 cannot be used by another group.

Examples

# Configure a service object with a protocol number of **100**.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service 100
```

# Configure a service object with the source and destination port numbers for the TCP service.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service tcp source eq 100 destination range 10 100
```

# Configure a service object with the message type and code for the ICMP service.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service icmp 100 150
```

# Configure a service object using object group **servicegroup2**.

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-port-portgroup] service group-object servicegroup2
```

New feature: Maximum number of retransmission attempts for control packets

Setting the maximum number of retransmission attempts for control packets

The intervals for the first five retransmission attempts are 1, 2, 4, 8, and 16. The maximum retransmission interval is 16. After the interval reaches 16, the intervals for subsequent retransmission attempts remain 16. If the number of retransmission attempts reaches the limit, the tunnel is deleted.

To set the maximum number of retransmission attempts for control packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter L2TP group view.	**l2tp-group** *group-number* [**mode** { **lac** | **lns** }]	N/A
3. Set the maximum number of retransmission attempts for control packets.	**tunnel retransmit** *value*	By default, the maximum number of retransmission attempts is 16.

Command reference

tunnel retransmit

Use **tunnel retransmit** to set the maximum number of retransmission attempts for control packets.

Use **undo tunnel retransmit** to restore the default.

Syntax

tunnel retransmit *value*

undo tunnel retransmit

Default

The maximum number of retransmission attempts for control packets is 16.

Views

L2TP group view

Predefined user roles

network-admin

Parameters

value: Specifies the maximum number of retransmission attempts for control packets, in the range of 5 to 65535.

Usage guidelines

The intervals for the first five retransmission attempts are 1, 2, 4, 8, and 16. The maximum retransmission interval is 16. After the interval reaches 16, the intervals for subsequent retransmission attempts remain 16. If the number of retransmission attempts reaches the limit, the tunnel is deleted.

Examples

# Set the maximum number of retransmission attempts for control packets to 20.

```
<Sysname> system-view
[Sysname] l2tp-group 1 mode lac
[Sysname-l2tp1] tunnel retransmit 20
```

Modified feature: Maximum value for the Layer 3 aggregate interface number

Feature change description

The maximum value for the Layer 3 aggregate interface number was changed from 64 to 4096.

Command changes

The maximum value for the Layer 3 aggregate interface number was change from 64 to 4096 in the following commands:

- **display interface**
- **display link-aggregation load-sharing mode**
- **display link-aggregation verbose**
- **interface route-aggregation**
- **port link-aggregation group**
- **reset counters interface**

Modified feature: Support for inter-AS IPv6 VPN option B

Feature change description

This release added support for the inter-AS IPv6 VPN option B solution.

Command changes

None.

Modified feature: Advertising the COMMUNITY attribute to a peer or peer group in BGP VPNv6 address family view or BGP-VPN IPv6 unicast address family view

Feature change description

This release added support for advertising the COMMUNITY attribute to a peer or peer group in BGP VPNv6 address family view and BGP-VPN IPv6 unicast address family view.

Command changes

Modified command: peer advertise-community

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP VPNv4 address family view/BGP VPNv6 address family view/BGP IPv4 multicast address family view:

peer { *group-name* **|** *ip-address* } **advertise-community**

undo peer { *group-name* **|** *ip-address* } **advertise-community**

In BGP IPv6 unicast address family view:

peer { *group-name* **|** *ip-address* **|** *ipv6-address* } **advertise-community**

undo peer { *group-name* **|** *ip-address* **|** *ipv6-address* } **advertise-community**

In BGP IPv6 multicast address family view/BGP-VPN IPv6 unicast address family view:

peer { *group-name* **|** *ipv6-address* } **advertise-community**

undo peer { *group-name* **|** *ipv6-address* } **advertise-community**

Views

BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, BGP VPNv4 address family view, BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, BGP VPNv6 address family view, BGP IPv4 multicast address family view, BGP IPv6 multicast address family view

Change description

This release added support for the command in BGP VPNv6 address family view and BGP-VPN IPv6 unicast address family view.

Modified feature: Configuring manual route summarization in BGP-VPN IPv6 unicast address family view

Feature change description

This release added support for configuring manual route summarization in BGP-VPN IPv6 unicast address family view.

Command changes

Modified command: aggregate

Syntax

In BGP IPv4 unicast address family view/BGP-VPN IPv4 unicast address family view/BGP IPv4 multicast address family view:

aggregate *ip-address* { *mask* **|** *mask-length* } [**as-set** **|** **attribute-policy** *route-policy-name* **|** **detail-suppressed** **|** **origin-policy** *route-policy-name* **|** **suppress-policy** *route-policy-name*] *

undo aggregate *ip-address* { *mask* **|** *mask-length* }

In BGP IPv6 unicast address family view/BGP-VPN IPv6 unicast address family view/BGP IPv6 multicast address family view:

aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ipv6-address prefix-length*

Views

BGP IPv4 unicast address family view, BGP-VPN IPv4 unicast address family view, BGP IPv6 unicast address family view, BGP-VPN IPv6 unicast address family view, BGP IPv4 multicast address family view, BGP IPv6 multicast address family view

Change description

This release added support for the command in BGP-VPN IPv6 unicast address family view.

Modified feature: Setting the OSPF SPF calculation interval

Feature change description

This release added support for setting the fixed OSPF SPF calculation interval.

Command changes

Modified command: spf-schedule-interval

Old syntax

spf-schedule-interval *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

New syntax

spf-schedule-interval { *maximum-interval* [*minimum-interval* [*incremental-interval*]] **| millisecond** *interval* }

undo spf-schedule-interval

Views

OSPF view

Change description

Before modification: The **millisecond** *interval* option is not supported.

After modification: The **millisecond** *interval* option is supported.

Modified feature: Setting the LSU transmission interval

Feature change description

The value range for the interval at which an interface sends LSU packets was changed to 0 to 1000.

Command changes

Modified command: transmit-pacing

Syntax

transmit-pacing interval *interval* **count** *count*

undo transmit-pacing

Views

OSPF view

Change description

Before modification: The value range for the *interval* argument is 10 to 1000 milliseconds.

After modification: The value range for the *interval* argument is 0 to 1000 milliseconds.

Modified feature: ACL rules support object groups

Feature change description

Support for object groups was added to the IPv4 basic and advanced ACL rules and the IPv6 basic and advanced ACL rules.

Command changes

Modified command: rule (IPv4 advanced ACL view)

Old syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

New syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Views

IPv4 advanced ACL view

Change description

Before modification: The command does not support the **object-group** *address-group-name* and **object-group** *port-group-name* options.

After modification: The command supports the **object-group** *address-group-name* and **object-group** *port-group-name* options.

Modified command: rule (IPv4 basic ACL view)

Old syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

New syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Views

IPv4 basic ACL view

Change description

Before modification: The command does not support the **object-group** *address-group-name* option.

After modification: The command supports the **object-group** *address-group-name* option.

Modified command: rule (IPv6 advanced ACL view)

Old syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

New syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Views

IPv6 advanced ACL view

Change description

Before modification: The command does not support the **object-group** *address-group-name* and **object-group** *port-group-name* options.

After modification: The command supports the **object-group** *address-group-name* and **object-group** *port-group-name* options.

Modified command: rule (IPv6 basic ACL view)

Old syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

New syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address*/*source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

Views

IPv6 basic ACL view

Change description

Before modification: The command does not support the **object-group** *address-group-name* option.

After modification: The command supports the **object-group** *address-group-name* option.

R7103P05

This release has the following changes:

- New feature: BFD for an aggregation group
- New feature: Marking the EXP value in the second label of MPLS packets
- New feature: Support of PPP for configuring the PPP usernames as the client IDs
- Modified feature: Configuring the local PE (RR) to not change the next hop of VPNv4 or VPNv6 routes advertised to BGP peers (RR clients)
- New feature: Link-aggregation load sharing enhancement for MPLS packets in an aggregation group
- New feature: Support of link aggregation for specifying a backup traffic processing card for a Layer 3 aggregate interface
- New feature: Support of PPP for specifying a backup traffic processing card for VA interfaces on a VT interface
- New feature: Support of L2TP for specifying a backup traffic processing card for a virtual PPP interface
- New feature: Support of HDLC for specifying a backup traffic processing card for an HDLC link bundle interface
- New feature: Ignoring IGP metrics during optimal route selection
- Modified feature: Support for assigning Layer 3 Ethernet subinterfaces to Layer 3 aggregation groups and configuring dynamic link aggregation commands in Layer 3 Ethernet subinterface view
- Modified feature: Setting the global and group-specific load sharing modes
- Modified feature: Enabling PPP LQM to send LCP echo packets upon detecting low quality links
- Modified feature: Displaying information about temporary L2TP sessions
- Modified feature: Creating a BFD session for detecting the local interface state
- Modified feature: Removing the Router Alert option from BFD packets for LSP connectivity verification
- Modified feature: Configuring the local PE (RR) to not change the next hop of VPNv4 or VPNv6 routes advertised to BGP peers (RR clients)

New feature: BFD for an aggregation group

Enabling BFD for an aggregation group

BFD for Ethernet link aggregation can monitor member link status in an aggregation group. After you enable BFD on an aggregate interface, each Selected port in the aggregation group establishes a BFD session with its peer port. BFD operates differently depending on the aggregation mode.

- **BFD for static aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. The local port is placed in Unselected state. The BFD session between the local and peer ports remains, and the local port keeps sending BFD packets. When the link is recovered, the local port receives BFD packets from the peer port, and BFD notifies the Ethernet link aggregation module that the peer port is reachable. The local port is placed in the Selected state again. This mechanism ensures that the local and peer ports of a static aggregate link have the same aggregation state.
- **BFD for dynamic aggregation**—When BFD detects a link failure, BFD notifies the Ethernet link aggregation module that the peer port is unreachable. BFD clears the session and stops

sending BFD packets. When the link is recovered and the local port is placed in Selected state again, the local port establishes a new session with the peer port. BFD notifies the Ethernet link aggregation module that the peer port is reachable. Because BFD provides fast failure detection, the local and peer systems of a dynamic aggregate link can negotiate the aggregation state of their member ports faster.

For more information about BFD, see *High Availability Configuration Guide*.

Configuration restrictions and guidelines

When you enable BFD for an aggregation group, follow these restrictions and guidelines:

- Make sure the source and destination IP addresses are consistent at the two ends of an aggregate link. For example, if you execute **link-aggregation bfd ipv4 source** 1.1.1.1 **destination** 2.2.2.2 on the local end, execute **link-aggregation bfd ipv4 source** 2.2.2.2 **destination** 1.1.1.1 on the peer end.
- The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group.
- Hewlett Packard Enterprise recommends not configuring other protocols to collaborate with BFD on a BFD-enabled aggregate interface.

Configuration procedure

To enable BFD for an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	N/A
3. Enable BFD for the aggregation group.	**link-aggregation bfd ipv4 source** *ip-address* **destination** *ip-address*	By default, BFD is disabled for an aggregation group. The source and destination IP addresses of BFD sessions must be unicast addresses excluding 0.0.0.0.

Command reference

link-aggregation bfd ipv4

Use **link-aggregation bfd ipv4** to enable BFD for an aggregation group.

Use **undo link-aggregation bfd** to disable BFD for an aggregation group.

Syntax

link-aggregation bfd ipv4 source *ip-address* **destination** *ip-address*

undo link-aggregation bfd

Default

BFD is disabled for an aggregation group.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

source *ip-address*: Specifies the source IP address of BFD sessions.

destination *ip-address*: Specifies the destination IP address of BFD sessions.

Examples

# Enable BFD for Layer 3 aggregation group 1, and specify the source and destination IP addresses as 1.1.1.1 and 2.2.2.2 for BFD sessions.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation bfd ipv4 source 1.1.1.1 destination 2.2.2.2
```

New feature: Marking the EXP value in the second label of MPLS packets

Configuring MPLS priority marking

In an MPLS network, you can adjust the priority of an MPLS traffic flow by marking its EXP value. For more information about priority marking, see *ACL and QoS Configuration Guide*.

To configure MPLS priority marking:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic class and enter traffic class view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic classes exist.
3. Configure match criteria for the traffic class.	• To match the EXP value in the first (topmost) label: **if-match** [**not**] **mpls-exp** *exp-value*&<1-8> • To match the EXP value in the second label: **if-match** [**not**] **second-mpls-exp** *exp-value*&<1-8>	By default, no match criteria are configured. The match criteria apply only to MPLS packets.
4. Return to system view.	**quit**	N/A
5. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	By default, no traffic behaviors exist.
6. Configure an EXP marking action in the traffic behavior.	• For the first (topmost) label: **remark mpls-exp** *exp-value* • For the second label: **remark second-mpls-exp** *exp-value*	By default, no EXP marking action is configured.

Step	Command	Remarks
7. Return to system view.	**quit**	N/A
8. Create a QoS policy and enter QoS policy view.	**qos policy** *policy-name*	By default, no QoS policies exist.
9. Associate the traffic class with the traffic behavior in the QoS policy.	**classifier** *classifier-name* **behavior** *behavior-name*	By default, no traffic behavior is associated with a traffic class.
10. Return to system view.	**quit**	N/A
11. Apply the QoS policy.	You can apply a QoS policy to an interface or a control plane. For more information, see *ACL and QoS Configuration Guide.*	By default, no QoS policy is applied.

Command reference

if-match second-mpls-exp

Use **if-match second-mpls-exp** to define a criterion to match the EXP field in the second MPLS label.

Use **undo if-match second-mpls-exp** to delete the match criterion.

Syntax

if-match [**not**] **second-mpls-exp** *exp-value*&<1-8>

undo if-match [**not**] **second-mpls-exp** *exp-value*&<1-8>

Default

No criterion is defined to match the EXP field in the second MPLS label.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

not: Matches packets not conforming to the specified criterion.

exp-value&<1-8>: Specifies a space-separated list of up to eight EXP values. The value range for the *exp-value* argument is 0 to 7. If the same MPLS EXP value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.

Examples

# Define a criterion to match packets with EXP value 3 or 4 in the second MPLS label.

```
<Sysname> system-view
[Sysname] traffic classifier database
[Sysname-classifier-database] if-match second-mpls-exp 3 4
```

remark second-mpls-exp

Use **remark second-mpls-exp** to configure an EXP value marking action for the second MPLS label in a traffic behavior.

Use **undo remark second-mpls-exp** to delete the action.

Syntax

remark second-mpls-exp *exp-value*

undo remark second-mpls-exp

Default

No EXP value marking action is configured for the second MPLS label.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

exp-value: Specifies an EXP value in the range of 0 to 7.

Examples

# Set the EXP value to 0 for the second label of MPLS packets.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark second-mpls-exp 0
```

New feature: Support of PPP for configuring the PPP usernames as the client IDs

Configuring PPP usernames as the client IDs

To enable a DHCP address pool to assign IP addresses to PPP users, you can configure PPP usernames as client IDs first.

To configure the device as the server (Specify a DHCP address pool):

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure DHCP.	• If the server acts as a DHCP server, perform the following tasks: ○ Configure the DHCP server. ○ Configure a DHCP address pool on the server. • If the server acts as a DHCP relay agent, perform the following tasks: ○ Configure the DHCP relay agent on the server.	For more information about DHCP, see *Layer 3—IP Services Configuration Guide*.

Step	Command	Remarks
	○ Configure a DHCP address pool on the remote DHCP server. ○ Enable the DHCP relay agent to record relay entries. ○ Configure a DHCP relay address pool.	
3. Enter interface view.	**interface** *interface-type interface-number*	N/A
4. Configure the interface to assign an IP address from the configured DHCP address pool to the peer.	**remote address pool** *pool-name*	By default, an interface does not assign an IP address to the peer.
5. Configure an IP address for the interface.	**ip address** *ip-address*	By default, no IP address is configured on an interface.
6. (Optional.) Use the PPP usernames as the DHCP client IDs.	**remote address dhcp client-identifier username**	By default, the PPP usernames are not used as the DHCP client IDs.

To configure the device as the server (Associate a DHCP address pool with an ISP domain):

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure DHCP.	• If the server acts as a DHCP server, perform the following tasks: ○ Configure the DHCP server. ○ Configure a DHCP address pool on the server. • If the server acts as a DHCP relay agent, perform the following tasks: ○ Configure the DHCP relay agent on the server. ○ Configure a DHCP address pool on the remote DHCP server. ○ Enable the DHCP relay agent to record relay entries. ○ Configure a DHCP relay address pool.	For more information about DHCP, see *Layer 3—IP Services Configuration Guide*.
3. Enter ISP domain view.	**domain** *isp-name*	N/A
4. Associate the ISP domain with the configured DHCP address pool for address assignment.	**authorization-attribute ip-pool** *pool-name*	By default, no DHCP address pool is associated. For more information about this command, see AAA in *Security Command Reference*.
5. Return to system view.	**quit**	N/A
6. Enter interface view.	**interface** *interface-type*	N/A

Step	Command	Remarks
	interface-number	
7. Configure an IP address for the interface.	**ip address** *ip-address*	By default, no IP address is configured on an interface.
8. (Optional.) Use the PPP usernames as the DHCP client IDs.	**remote address dhcp client-identifier username**	By default, the PPP usernames are not used as the DHCP client IDs.

Command reference

remote address dhcp client-identifier

Use **remote address dhcp client-identifier username** to configure the PPP usernames as the DHCP client IDs.

Use **undo remote address dhcp client-identifier** to restore the default.

Syntax

remote address dhcp client-identifier username

undo remote address dhcp client-identifier

Default

The PPP usernames are not used as the DHCP client IDs.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

This command configures PPP usernames as DHCP client IDs for DHCP pool address assignment. The DHCP pool can be an AAA-authorized address pool or an address pool configured by using the **remote address** command.

Examples

# Configure the PPP usernames as the DHCP client IDs on Serial 2/1/0.

```
<Sysname> system-view
[Sysname] interface serial 2/1/0
[Sysname-Serial2/1/0] remote address dhcp client-identifier username
```

New feature: Link-aggregation load sharing enhancement for MPLS packets in an aggregation group

Enabling link-aggregation load sharing enhancement for MPLS packets in an aggregation group

This feature enables an aggregation group to use the five-tuple to identify data flows of MPLS packets and load share the packets. The five-tuple contains the source IP address, source port number, destination IP address, destination port number, and protocol number. This feature is available only on the provider (P) device. For information about the P device, see MPLS L3VPN in *MPLS Configuration Guide*.

To enable link-aggregation load sharing enhancement for MPLS packets in an aggregation group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	N/A
3. Enable link-aggregation load sharing enhancement for MPLS packets.	**link-aggregation load-sharing mpls enhanced**	By default, link-aggregation load sharing enhancement is disabled for MPLS packets in an aggregation group.

Command reference

link-aggregation load-sharing mpls enhanced

Use **link-aggregation load-sharing mpls enhanced** to enable link-aggregation load sharing enhancement for MPLS packets in an aggregation group.

Use **undo link-aggregation load-sharing mpls enhanced** to disable link-aggregation load sharing enhancement for MPLS packets in an aggregation group.

Syntax

link-aggregation load-sharing mpls enhanced

undo link-aggregation load-sharing mpls enhanced

Default

Link-aggregation load sharing enhancement is disabled for MPLS packets in an aggregation group.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Examples

# Enable link-aggregation load sharing enhancement for MPLS packets in Layer 3 aggregation group 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation load-sharing mpls enhanced
```

New feature: Support of link aggregation for specifying a backup traffic processing card for a Layer 3 aggregate interface

Specifying a backup traffic processing card for a Layer 3 aggregate interface

Specify a traffic processing card for a Layer 3 aggregate interface if all traffic on the Layer 3 aggregate interface is required to be processed on the same card.

For high availability, you can specify one primary and one backup traffic processing card by using the **service** command and the **service standby** command, respectively.

To specify a backup traffic processing card for a Layer 3 aggregate interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	N/A
3. Specify a backup traffic processing card for the Layer 3 aggregate interface.	• In standalone mode: **service standby slot** *slot-number* • In IRF mode: **service standby chassis** *chassis-number* **slot** *slot-number*	By default, no backup traffic processing card is specified.

Command reference

service standby

Use **service standby** to specify a backup traffic processing card for a Layer 3 aggregate interface.

Use **undo service standby** to restore the default.

Syntax

In standalone mode:

service standby slot *slot-number*

undo service standby slot

In IRF mode:

service standby chassis *chassis-number* **slot** *slot-number*

undo service standby chassis

Default

No backup traffic processing card is specified.

Views

Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies a card by its slot number. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (In IRF mode.)

Usage guidelines

Specify traffic processing cards if all traffic on a Layer 3 aggregate interface is required to be processed on the same card. If you do not specify a traffic processing card for a Layer 3 aggregate interface, traffic on that interface is processed by the card at which the traffic arrives.

For high availability, you can specify one primary and one backup traffic processing card by using the **service** command and the **service standby** command, respectively. The primary and backup cards must be different cards.

To avoid processing card switchover, specify the primary card before specifying the backup card. If you specify the backup card before specifying the primary card, traffic is switched over to the primary card immediately after you specify the primary card.

If you specify both primary and backup cards, the backup card takes over when the primary card becomes unavailable. The backup card continues to process traffic for the interface after the primary card becomes available again. The switchover will not occur until the backup card becomes unavailable.

When no specified traffic processing cards are available, the device does not drop the traffic on the Layer 3 aggregate interface if the interface is up. Instead, the traffic is processed by the card at which it arrives. Then, the specified processing card that first becomes available again takes over.

Examples

# (In standalone mode.) Specify the card in slot 2 as the primary traffic processing card for Layer 3 aggregate interface Route-Aggregation 1. Specify the card in slot 3 as the backup traffic processing card for Layer 3 aggregate interface Route-Aggregation 1.

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] service slot 2
[Sysname-Route-Aggregation1] service standby slot 3
```

New feature: Support of PPP for specifying a backup traffic processing card for VA interfaces on a VT interface

Specifying a backup traffic processing card for VA interfaces on a VT interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a VT interface and enter its view.	**interface virtual-template** *number*	If the VT interface already exists, you enter its view directly.
3. Specify a backup traffic processing card for the VA interfaces of the VT interface.	• In standalone mode: **service standby slot** *slot-number* • In IRF mode: **service standby chassis** *chassis-number* **slot** *slot-number*	By default, no backup traffic processing card is specified.

Command reference

service standby

Use **service standby** to specify a backup traffic processing card for VA interfaces on a VT interface.

Use **undo service standby** to restore the default.

Syntax

In standalone mode:

service standby slot *slot-number*

undo service standby slot

In IRF mode:

service standby chassis *chassis-number* **slot** *slot-number*

undo service standby chassis

Default

No backup traffic processing card is specified.

Views

VT interface view

Default command level

network-admin

Parameters

slot s*lot-number*: Specifies a card by its slot number. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (In IRF mode.)

Usage guidelines

If you do not specify a traffic processing card for VA interfaces on a VT interface, traffic on that interface is processed by the card at which the traffic arrives.

For high availability, you can specify one primary and one backup traffic processing card by using the **service** command and the **service standby** command, respectively. The primary and backup cards must be different cards.

To avoid processing card switchover, specify the primary card before specifying the backup card. If you specify the backup card before specifying the primary card, traffic is switched over to the primary card immediately after you specify the primary card.

If you specify both primary and backup cards, the backup card takes over when the primary card becomes unavailable. The backup card continues to process traffic for the interface after the primary card becomes available again. The switchover will not occur until the backup card becomes unavailable.

When no specified traffic processing cards are available, the traffic is processed by the card at which it arrives. Then, the specified processing card that first becomes available again takes over.

Examples

# (In standalone mode.) Specify the card in slot 2 as the primary traffic processing card for the VA interfaces on interface Virtual-Template 10. Specify the card in slot 3 as the backup traffic processing card for the VA interfaces on interface Virtual-Template 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] service slot 2
[Sysname-Virtual-Template10] service standby slot 3
```

# (In IRF mode.) Specify the card in slot 2 of IRF member device 2 as the primary traffic processing card for the VA interfaces on interface Virtual-Template 10. Specify the card in slot 3 of IRF member device 2 as the backup traffic processing card for the VA interfaces on interface Virtual-Template 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] service chassis 2 slot 2
[Sysname-Virtual-Template10] service standby chassis 2 slot 3
```

New feature: Support of L2TP for specifying a backup traffic processing card for a virtual PPP interface

Specifying a backup traffic processing card for a virtual PPP interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a virtual PPP interface and enter its view.	**interface virtual-ppp** *interface-number*	By default, no virtual PPP interface exists.
3. Specify a backup traffic processing card for the virtual PPP interface.	• In standalone mode: **service standby slot** *slot-number* • In IRF mode: **service standby chassis** *chassis-number* **slot** *slot-number*	By default, no backup traffic processing card is specified.

Command reference

service standby

Use **service standby** to specify a backup traffic processing card for a virtual PPP interface.

Use **undo service standby** to restore the default.

Syntax

In standalone mode:

service standby slot *slot-number*

undo service standby slot

In IRF mode:

service standby chassis *chassis-number* **slot** *slot-number*

undo service standby chassis

Default

No backup traffic processing card is specified.

Views

Virtual PPP interface view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies a card by its slot number. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (In IRF mode.)

Usage guidelines

The **service standby** command affects only L2TP data messages. The control messages are always processed on the active MPU.

Specify traffic processing cards if flow control is enabled. If you do not specify a traffic processing card for a virtual PPP interface, traffic on that interface is processed by the card at which the traffic arrives.

For high availability, you can specify one primary and one backup traffic processing card by using the **service** command and the **service standby** command, respectively. The primary and backup cards must be different cards.

To avoid processing card switchover, specify the primary card before specifying the backup card. If you specify the backup card before specifying the primary card, traffic is switched over to the primary card immediately after you specify the primary card.

If you specify both primary and backup cards, the backup card takes over when the primary card becomes unavailable. The backup card continues to process traffic for the interface after the primary card becomes available again. The switchover will not occur until the backup card becomes unavailable.

When no specified traffic processing cards are available, the device does not drop the traffic on the virtual PPP interface if the interface is up. Instead, the traffic is processed by the card at which it arrives. Then, the specified processing card that first becomes available again takes over.

Examples

# (In standalone mode.) Specify the card in slot 2 as the primary traffic processing card for interface Virtual-PPP 10. Specify the card in slot 3 as the backup traffic processing card for interface Virtual-PPP 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] service slot 2
[Sysname-Virtual-PPP10] service standby slot 3
```

# (In IRF mode.) Specify the card in slot 2 on IRF member device 2 as the primary traffic processing card for interface Virtual-PPP 10. Specify the card in slot 3 on IRF member device 2 as the backup traffic processing card for interface Virtual-PPP 10.

```
<Sysname> system-view
[Sysname] interface virtual-ppp 10
[Sysname-Virtual-PPP10] service chassis 2 slot 2
[Sysname-Virtual-PPP10] service standby chassis 2 slot 3
```

New feature: Support of HDLC for specifying a backup traffic processing card for an HDLC link bundle interface

Specifying a backup traffic processing card for an HDLC link bundle interface

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an HDLC link bundle interface and enter its view.	**interface hdlc-bundle** *bundle-id*	By default, no HDLC link bundle interface exists.
3. Specify a backup traffic processing card for the HDLC link bundle interface.	• In standalone mode: **service standby slot** *slot-number* • In IRF mode:	By default, no backup traffic processing card is specified.

Step	Command	Remarks
	service standby chassis *chassis-number* **slot** *slot-number*	

Command reference

service standby

Use **service standby** to specify a backup traffic processing card for an HDLC link bundle interface.

Use **undo service standby** to restore the default.

Syntax

In standalone mode:

service standby slot *slot-number*

undo service standby slot

In IRF mode:

service standby chassis *chassis-number* **slot** *slot-number*

undo service standby chassis

Default

No backup traffic processing card is specified.

Views

HDLC link bundle interface view

Default command level

network-admin

Parameters

slot s*lot-number*: Specifies a card by its slot number. (In standalone mode.)

chassis *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device. The *chassis-number* argument represents the member ID of the IRF member device. The *slot-number* argument represents the slot number of the card. (In IRF mode.)

Usage guidelines

If you do not specify a traffic processing card for an HDLC link bundle interface, traffic on that interface is processed by the card at which the traffic arrives.

For high availability, you can specify one primary and one backup traffic processing card by using the **service** command and the **service standby** command, respectively. The primary and backup cards must be different cards.

To avoid processing card switchover, specify the primary card before specifying the backup card. If you specify the backup card before specifying the primary card, traffic is switched over to the primary card immediately after you specify the primary card.

If you specify both primary and backup cards, the backup card takes over when the primary card becomes unavailable. The backup card continues to process traffic for the interface after the primary card becomes available again. The switchover will not occur until the backup card becomes unavailable.

When no specified traffic processing cards are available, the device does not drop the traffic on the HDLC link bundle interface if the interface is up. Instead, the traffic is processed by the card at which it arrives. Then, the specified processing card that first becomes available again takes over.

Examples

# (In standalone mode.) Specify the card in slot 2 as the primary traffic processing card for HDLC link bundle interface 1. Specify the card in slot 3 as the backup traffic processing card for HDLC link bundle interface 1.

```
<Sysname> system-view
[Sysname] interface hdlc-bundle 1
[Sysname-HDLC-bundle1] service slot 2
[Sysname-HDLC-bundle1] service standby slot 3
```

# (In IRF mode.) Specify the card in slot 2 of member device 2 as the primary traffic processing card for HDLC link bundle interface 1. Specify the card in slot 3 of member device 2 as the backup traffic processing card for HDLC link bundle interface 1.

```
<Sysname> system-view
[Sysname] interface hdlc-bundle 1
[Sysname-HDLC-bundle1] service chassis 2 slot 2
[Sysname-HDLC-bundle1] service standby chassis 2 slot 3
```

New feature: Ignoring IGP metrics during optimal route selection

Ignoring IGP metrics during optimal route selection

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter BGP instance view or BGP-VPN instance view.	- Enter BGP instance view: **bgp** *as-number* [**instance** *instance-name*] - Enter BGP-VPN instance view: **a.** **bgp** *as-number* [**instance** *instance-name*] **b.** **ip vpn-instance** *vpn-instance-name*	N/A
3. Configure BGP to ignore IGP metrics during optimal route selection.	**bestroute igp-metric-ignore**	By default, BGP considers IGP metrics during optimal route selection. If multiple routes to the same destination are available, BGP selects the route with the smallest IGP metric as the optimal route.

Command reference

bestroute igp-metric-ignore

Use **bestroute igp-metric-ignore** to configure BGP to ignore IGP metrics during optimal route selection.

Use **undo bestroute igp-metric-ignore** to restore the default.

Syntax

bestroute igp-metric-ignore

undo bestroute igp-metric-ignore

Default

BGP considers IGP metrics during optimal route selection, and selects the route with the smallest IGP metric as the optimal route.

Views

BGP instance view, BGP-VPN instance view

Predefined user roles

network-admin

mdc-admin

Examples

# In BGP instance view of BGP instance **default**, ignore IGP metrics during optimal route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] bestroute igp-metric-ignore
```

Modified feature: Support for assigning Layer 3 Ethernet subinterfaces to Layer 3 aggregation groups and configuring dynamic link aggregation commands in Layer 3 Ethernet subinterface view

Feature change description

This release added support for the following commands in Layer 3 Ethernet subinterface view:

- **lacp mode**
- **lacp period short**
- **link-aggregation port-priority**
- **port link-aggregation group**

Command changes

Modified command: lacp mode

Syntax

lacp mode passive

undo lacp mode

Views

Layer 3 Ethernet interface view, Layer 3 Ethernet subinterface view

Change description

Layer 3 Ethernet subinterface view was added.

Modified command: lacp period short

Syntax

lacp period short

undo lacp period

Views

Layer 3 Ethernet interface view, Layer 3 Ethernet subinterface view

Change description

Layer 3 Ethernet subinterface view was added.

Modified command: link-aggregation port-priority

Syntax

link-aggregation port-priority *port-priority*

undo link-aggregation port-priority

Views

Layer 3 Ethernet interface view, Layer 3 Ethernet subinterface view

Change description

Layer 3 Ethernet subinterface view was added.

Modified command: port link-aggregation group

Syntax

port link-aggregation group *number*

Views

Layer 3 Ethernet interface view, Layer 3 Ethernet subinterface view

Change description

Layer 3 Ethernet subinterface view was added.

Modified feature: Setting the global and group-specific load sharing modes

Feature change description

The syntax was changed for the **link-aggregation global load-sharing mode** and **link-aggregation load-sharing mode** commands.

Command changes

Modified command: link-aggregation global load-sharing mode

Old syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** | **bandwidth-usage** | **per-packet** }

New syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** | **per-packet** }

Views

System view

Change description

The **bandwidth-usage** keyword was deleted.

Modified command: link-aggregation load-sharing mode

Old syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** | **per-packet** }

New syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-port** | **ip-protocol** | **mpls-label1** | **mpls-label2** | **mpls-label3** | **source-ip** | **source-port** | **per-packet** | **bandwidth-usage** }

Views

Layer 3 aggregate interface view

Change description

The **destination-mac** and **source-mac** keywords were deleted and the following keywords were added:

- **destination-port**: Load shares traffic based on destination ports.
- **ip-protocol**: Load shares traffic based on IP protocol types.
- **mpls-label1**: Load shares MPLS traffic based on Layer 1 labels.
- **mpls-label2**: Load shares MPLS traffic based on Layer 2 labels.
- **mpls-label3**: Load shares MPLS traffic based on Layer 3 labels.
- **source-port**: Load shares traffic based on source ports.
- **bandwidth-usage**: Load shares traffic based on bandwidth usage.

Modified feature: Enabling PPP LQM to send LCP echo packets upon detecting low quality links

Feature change description

PPP LQM can periodically send large LCP echo packets upon detecting low quality links.

Command changes

New command: ppp lqm lcp-echo

Use **ppp lqm lcp-echo** to enable LQM to send LCP echo packets upon detecting low quality links.

Use **undo ppp lqm lcp-echo** to restore the default.

Syntax

ppp lqm lcp-echo [**packet** *size*] [**interval** *seconds*]

undo ppp lqm lcp-echo

Default

LQM does not send LCP echo packets upon detecting a low quality link.

Views

Interface view

Predefined user roles

network-admin

Parameters

packet *size*: Specifies the LCP echo packet size in the range of 128 to 1500 bytes.

interval *seconds*: Specifies the LCP echo interval in the range of 1 to 10 seconds.

Usage guidelines

After you enable PPP LQM, you can use this command to enable LQM to periodically send large LCP echo packets upon detecting low quality links. This feature prevents link flapping on low quality links caused by large packets.

Examples

# Enable Serial 2/1/1 to send a 1400-byte LCP echo packet every one second upon detecting low quality links.

```
<Sysname> system-view
[Sysname] interface serial 2/1/1
[Sysname-Serial2/1/1] ppp lqm lcp-echo packet 1400 interval 1
```

Modified feature: Displaying information about temporary L2TP sessions

Feature change description

L2TP supports displaying information about temporary L2TP sessions.

Command changes

New command: display l2tp session temporary

Use **display l2tp session temporary** to display information about temporary L2TP sessions.

Syntax

display l2tp session temporary

Views

Any view

Predefined user roles

network-admin

mdc-admin

Examples

# Display information about temporary L2TP sessions.

```
<Sysname> display l2tp session temporary
Total number of temporary sessions: 6
LocalSID    RemoteSID    LocalTID    State
2298        0            19699       Wait-tunnel
42805       0            19699       Wait-tunnel
17777       0            19699       Wait-tunnel
58284       0            19699       Wait-tunnel
33256       0            19699       Wait-tunnel
8228        0            19699       Wait-tunnel
```

Table 1 Command output

Field	Description
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
State	Session state:

Field	Description
	• **Idle**. • **Wait-tunnel**—Waits for the tunnel to be established. • **Wait-reply**—Waits for an Incoming-Call-Reply (ICRP) message indicating the call is accepted. • **Wait-connect**—Waits for an Incoming-Call-Connected (ICCN) message.

Modified feature: Creating a BFD session for detecting the local interface state

Feature change description

Layer 3 Ethernet subinterface view was added. For BFD detection to take effect, do not configure this feature on both a Layer 3 Ethernet interface and its subinterface.

Command changes

Modified command: bfd detect-interface

Syntax

bfd detect-interface source-ip *ip-address*

Views

Interface view

Change description

Before modification: The command is not supported in Layer 3 Ethernet subinterface view.

After modification: The command is supported in Layer 3 Ethernet subinterface view. For BFD detection to take effect, do not configure this feature on both a Layer 3 Ethernet interface and its subinterface.

Modified feature: Removing the Router Alert option from BFD packets for LSP connectivity verification

Feature change description

This release added support for removing the Router Alert option from BFD packets for LSP connectivity verification.

Command changes

New command: bfd ip-router-alert

Use **bfd ip-router-alert** to add the Router Alert option in BFD packets for LSP connectivity verification.

Use **undo bfd ip-router-alert** to remove the Router Alert option from BFD packets for LSP connectivity verification.

Syntax

bfd ip-router-alert

undo bfd ip-router-alert

Default

The device adds the Router Alert option in BFD packets for LSP connectivity verification.

Views

System view

Predefined user roles

network-admin

network-operator

Usage guidelines

Execute the **undo bfd ip-router-alert** command on the local device if the peer device cannot identify the Router Alert option in BFD packets.

This command does not take effect for a BFD session whose state is up before this command is executed.

Examples

# Remove the Router Alert option from BFD packets.

```
<Sysname> system-view
[Sysname] undo bfd ip-router-alert
```

Modified feature: Configuring the local PE (RR) to not change the next hop of VPNv4 or VPNv6 routes advertised to BGP peers (RR clients)

Feature change description

This release added support for the local PE (RR) to not change the next hop of VPNv4/VPNv6 routes advertised to BGP peers (RR clients) in an inter-AS option C scenario.

Command changes

Modified command: peer next-hop-invariable

Syntax

peer { *group-name* **|** *ip-address* [*mask-length*] } **next-hop-invariable**

Views

BGP VPNv4 address family view, BGP VPNv6 address family view

Change description

Before modification: The **peer next-hop-invariable** command enables the device to not change the next hop of routes advertised to EBGP peers. This command is available only in BGP VPNv4 address family view.

After modification: The **peer next-hop-invariable** command enables the device to not change the next hop of routes advertised to BGP peers. This command is available in both BGP VPNv4 address family view and BGP VPNv6 address family view.