Hewlett Packard
Enterprise

HPE MSR954_MSR954P_MSR958-CMW710-R0411 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 R0411. 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 MSR954_MSR954P_MSR958-CMW710-R0411 Release Notes (Software Feature Changes) and the documents listed in "Related documents"

Version information

Version number

HPE Comware Software, Version 7.1.064, Release 0411

Please see the example below generated by the display version command:

```
<HPE> display version
HPE Comware Software, Version 7.1.064, Release 0411
Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP
HPE MSR954 uptime is 0 weeks, 0 days, 23 hours, 0 minutes
Last reboot reason : Power on
Boot image: flash:/msr954-cmw710-boot-r0411.bin
Boot image version: 7.1.064P21, Release 0411
  Compiled Jul 14 2016 16:00:00
System image: flash:/msr954-cmw710-system-r0411.bin
System image version: 7.1.064, Release 0411
  Compiled Jul 14 2016 16:00:00
Feature image(s) list:
  flash:/msr954-cmw710-wifidog-r0411.bin, version: 7.1.064
    Compiled Jul 14 2016 16:00:00
  flash:/msr954-cmw710-wwd-r0411.bin, version: 7.1.064
    Compiled Jul 14 2016 16:00:00
  flash:/msr954-cmw710-security-r0411.bin, version: 7.1.064
    Compiled Jul 14 2016 16:00:00
  flash:/msr954-cmw710-voice-r0411.bin, version: 7.1.064
    Compiled Jul 14 2016 16:00:00
  flash:/msr954-cmw710-data-r0411.bin, version: 7.1.064
    Compiled Jul 14 2016 16:00:00

CPU ID: 0xa
1G bytes DDR3 SDRAM Memory
10M bytes Flash Memory
PCB Version: 2.0
CPLD Version: 0.0
Basic BootWare Version: 1.41
Extended BootWare Version: 1.41
[SLOT 0]CON (Hardware)2.0, (Driver)1.0, (CPLD)0.0
[SLOT 0]GE0/0 (Hardware)2.0, (Driver)1.0, (CPLD)0.0
[SLOT 0]4GSW (Hardware)2.0, (Driver)1.0, (CPLD)0.0
[SLOT 0]SFP0/5 (Hardware)2.0, (Driver)1.0, (CPLD)0.0
[SLOT 0]CELLULAR0/0 (Hardware)2.0, (Driver)1.0, (CPLD)0.0
```

```
[SLOT 0]CELLULAR0/1 (Hardware)2.0, (Driver)1.0, (CPLD)0.0
```

Version history

Table 1 Version history

Version number	Last version	Release date	Release type	Remarks
CMW710-R0411	CMW710-R0410	2016-09-19	Release version	support MSR954_MSR954P_MSR958 series • Fixes bugs
CMW710-R0410	CMW710-R0408P05	2016-08-29	Release version	support MSR954_MSR954P_MSR958 series • New feature: 1. Support of multicast for ADVPN 2. Application layer state filtering 3.SIP keepalive 4.Multicast fast forwarding 5. Attack defense policy application to a security zone 6. AAA support for IKE extended authentication 7. Percentage-based CAR 8. Logging OSPF router ID conflict events 9.AFT 10. Configuring enhanced CC authentication in FIPS mode 11. Support of AAA for NETCONF 12. Mobile IP tunnel interface settings 13. LISP 14. LISP tunnel entries and dynamic mobility 15. Support of IPv6 multicast routing for VPN instances 16.LISP virtual machine multi-hop mobility and DDT 17. LISP NSR 18. PPPoE client support for IPv6 19. DPI engine and content filtering
	CMW710-R0304P12			

				20. IPS 21. NBAR 22. URL filtering 23. Local portal Web server 24.Support of portal for NETCONF 25. Newly-added MIB objects 26. IPS, ACG, and SSL VPN licenses 27. Support of NQA for NETCONF 28. Configuring CWMP to support VPN 29. Transceiver module source alarm 30. VLAN interface performance optimization 31. NAT support for multicast source address in PIM join/prune packets 32. GDOI GM group anti-replay window 33. SIP compatibility 34. Voice VLAN 35. L2TP-based EAD 36. BFD for an aggregation group 37. 4G modem IMSI/SN binding authentication 38. Media Stream Control (MSC) logging 39. IMSI/SN binding authentication 40. Specifying a band for a 4G modem 41. Using tunnel interfaces as OpenFlow ports 42. NETCONF support for ACL filtering 43. WAAS 44 Support for the MKI field in SRTP or SRTCP packets 45. SIP domain name 46. Setting the maximum size of advertisement files 47. Support of VCF for NETCONF

				48. Support of SNMP for NETCONF 49. Support of file system for NETCONF 50. Support of PoE for NETCONF 51. Support of RMON for NETCONF 52. Support of policy-based routing for NETCONF 53. Support of BGP for NETCONF 54. Support of OSPF for NETCONF 55. Support of ping for NETCONF 56. Support of tracert for NETCONF 57. Support of L2VPN for NETCONF 58. SIP support for VRF 59. IKEv2 60. Specifying an IKEv2 profile for an IPsec policy 61. Bidirectional BFD control detection for RIP 62. OSPF router ID autoconfiguration 63. Associating a static route with a track entry 64. VLAN tag processing rule for incoming traffic 65. IP-based portal-free rule 66. Portal redirect packet statistics 67. GDVPN 68. OpenFlow instance 69. Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set 70. Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy 71.SIP session refresh • Modified feature 1. User profile 2.Tunnel interface support for

				IPsec and VXLAN tunnel modes 3. PKI certificate auto-renewal 4. Configuring the PKI entity DN 5. ADVPN 6. Telnet redirect 7. DHCP snooping performance optimization 8. OSPF performance optimization 9. IP performance optimization 10. AAA 11. Configuring a cellular interface for a 3G/4G modem 12. QoS on VXLAN tunnel interfaces 13. Option 60 encapsulation in DHCP replies 14. MPLS QoS support for matching the EXP field 15. MPLS QoS support for marking the EXP field 16.Automatic configuration 17. User profile 18. Default size of the TCP receive and send buffer 19. Support for per-packet load sharing 20. Default user role 21. Debugging 22. SSH username 23. IS-IS hello packet sending interval 24. Displaying information about NTP servers from the reference source to the primary NTP server 25. Saving, rolling back, and loading the configuration 26. Displaying information about SSH users 27. SIP trusted nodes 28. IPsec ESP encryption algorithms 29. IPsec ESP authentication algorithms

				30. IPsec AH authentication algorithms 31. Specifying an encryption algorithm for an IKE proposal 32.Specifying an authentication algorithm for an IKE proposal 33. Generating asymmetric key pairs 34. Specifying an ECDSA key pair for certificate request 35. QoS MIB 36. Enabling PFS for an IPsec transform set 37. Displaying track entry infomration • Removed feature 1.Tiny proxy 2. Displaying switching fabric channel usage
CMW710-R0408P05	CMW710-R0407	2016-07-01	Release version	Only support MSR954P_MSR958 series • New feature: 1. BGP trap support for VRF information. 2. SSH redirect.
CMW710-R0407	CMW710-E0404P06	2016-05-11	Release version	Only support MSR954P_MSR958 series • Fixes bugs
CMW710-E0404P06	CMW710-E0403	2016-03-03	ESS version	Only support MSR954-D4G • Fixes bugs
CMW710-E0403	First release	2015-12-02	ESS version	Only support MSR954P_MSR958 series
CMW710-R0304P12	CMW710-E0304	2015-09-15	Release version	Only support MSR954
CMW710-E0304	First release	2015-06-11	ESS version	Only support MSR954

Hardware and software compatibility matrix

CAUTION:

To avoid an upgrade failure, use Table 3to verify the hardware and software compatibility before performing an upgrade.

Table 2 HPE product device numbers matrix

Product code	HPE MSR series
JH373A	HPE MSR954 Serial 1GbE Dual 4GLTE (WW) CWv7 Router

JH300A	HPE MSR958 1GbE Combo 2GbE-WAN 8GbE-LAN CWv7 Router
JH301A	HPE MSR958 1GbE Combo PoE+ 2GbE-WAN 8GbE-LAN CWv7 Router
JH296A	HP MSR954 1GbE+SFP Router
JH297A	HP MSR954-W 1GbE+SFP (WW) Router
JH298A	HP MSR954-W 1GbE+SFP LTE (AM) Rtr
JH299A	HP MSR954-W 1GbE+SFP LTE (WW) Rtr

Table 3 Hardware and software compatibility matrix

Item	Specifications			
Product family	MSR958 MSR954-D4G MSR954			
Boot ROM version	MSR958: 121 or higher MSR954-D4G: 120 or higher MSR954: 141 or higher			
Host software	Hardware	software	MD5 Check Sum	File size
	MSR958	MSR958-CMW710-R0411.IPE	5bca7ea9ed0353e006040843b61ae407	57,857,024 bytes
	MSR954-D4G	MSR954P-CMW710-R0411.IPE	3a2eb54228a8b2e4e2cc96629f6496bb	45,137,920 bytes
	MSR954	MSR954-CMW710-R0411.IPE	e3533740b11f183ed63958b8d23a1cc4	57,011,200 bytes
iMC version	iMC BIMS 7.2 (E0402P02) iMC EAD 7.2 (E0407) iMC TAM 7.2 (E0407) iMC UAM 7.2 (E0407) iMC MVM 7.2 (E0402P02) iMC NTA 7.2 (E0402P02) iMC PLAT 7.2 (E0403P04) iMC QoSM 7.2 (E0403H01) iMC RAM 7.2 (E0402) iMC SHM 7.2 (E0402I01) iMC UBA 7.2 (E0401p03) iMC VFM 7.2 (E0402H02)			
iNode version	iNode PC 7.2 (E0407)			

Upgrading restrictions and guidelines

None

Hardware feature updates

CMW710-R0411

None

Software feature and command updates

For more information about the software feature and command update history, see HPE MSR954_MSR954P_MSR958-CMW710-R0411 Release Notes (Software Feature Changes).

MIB updates

Table 4 MIB updates

Item	MIB file	Module	Description
CMW520-R0411			
New	None	None	None
Modified	None	None	None
CMW520-R0407			
New	None	None	None
Modified	hh3c-entity-ext.mib	HH3C-ENTITY-EXT-MIB	Added hh3cEntityExtSFPAlarmOnEx and hh3cEntityExtSFPAlarmOffEx of HH3C-ENTITY-EXT-MIB trap
	rfc1493-bridge.mib	BRIDGE-MIB	Modified description of dot1dTpFdbTable
	hh3c-splat-vlan.mib	HH3C-LswVLAN-MIB	Modified description of hh3cdot1qVlanType
	hh3c-pvst.mib	HH3C-PVST-MIB	Modified description of hh3cQinQv2IfConfigTable
	hh3c-qinqv2.mib	HH3C-QINQV2-MIB	Modified description of hh3cQinQv2ServiceTPID and hh3cQinQv2IfCustomerTPID
	hh3c-lpbkdt.mib	HH3C-LPBKDT-MIB	Modified description of Scalar objects and hh3cLpbkdtPortTable
	hh3c-power-eth-ext.mib	HH3C-POWER-ETH-EXT-MIB	Modified description of hh3cPseProfilePairs
	rfc3621-power-ethernet.mib	POWER-ETHERNET-MIB	Modified description of pethPsePortPowerPairs

Item	MIB file	Module	Description
	hh3c-splat-inf.mib	HH3C-LswINF-MIB	Modified description of hh3cifEthernetAutoSpeed
	hh3c-ifqos2.mib	HH3C-IFQOS2-MIB	Modified description of hh3cIfQoSLRConfigTable
CMW710-R0304P12			
New	None	None	None
Modified	rfc2925-disman-ping.mib	DISMAN-PING-MIB	Modified description of pingCtlTable
	hh3c-nqa.mib	HH3C-NQA-MIB	Modified description of hh3cNqaCtlTable
	hh3c-transceiver-info.mib	HH3C-TRANSCEIVER-INFO-MIB	Modified description of hh3cTransceiverCurTXPower and hh3cTransceiverCurRXPower

Operation changes

None

Restrictions and cautions

1. The WLAN configuration gets lost when the version of a router is degraded from E04XX or R04XX to R03XX. Please reconfigure WLAN features after degrading and save the configuration file.
2. The mGRE and Suite B features are not available in the current software version R04XX.

Open problems and workarounds

201608190045

- Symptom: Profile 3 of a VZW or Sprint modem cannot be modified.
- Condition: This symptom might occur if Profile 3 of a VZW or Sprint modem is modified.
- Workaround: None.

201608110569

- Symptom: The system executes commands issued through TR-069 from user view instead of from system view. As a result, command execution fails.
- Condition: This symptom might occur if the system executes commands issued through TR-069.
- Workaround: Add the **system-view** command to the beginning of the issued commands.

201607220244

- Symptom: The system displays a configuration success message when an IP address that is being used by a loopback interface is assigned to a GigabitEthernet interface through TR-069.

- Condition: This symptom might occur if an IP address that is being used by a loopback interface is assigned to a GigabitEthernet interface through TR-069.
- Workaround: Do not assign an IP address to multiple interfaces.

201607150391

- Symptom: The DHCP requests forwarded by a DHCP relay agent carry the IP address of the packet outgoing interface as the source IP address instead of the IP address of the DHCP relay interface.
- Condition: This symptom might occur if a DHCP relay agent forwards DHCP requests to the router that acts as a DHCP server.
- Workaround: Execute the **dhcp relay source-address x.x.x.x** command on the interface enabled with DHCP relay agent.

List of resolved problems

Resolved problems in CMW710-R0411

201609130134

- Symptom(1): CVE-2016-4953
- Condition(1): An attacker who knows the origin timestamp and can send a spoofed packet containing a CRYPTO-NAK to an ephemeral peer target before any other response is sent can demobilize that association.
- Symptom(2): CVE-2016-4954
- Condition(2): An attacker who is able to spoof packets with correct origin timestamps from enough servers before the expected response packets arrive at the target machine can affect some peer variables and, for example, cause a false leap indication to be set.
- Symptom(3): CVE-2016-4956
- Condition(3): The fix for NtpBug2978 does not cover broadcast associations, so broadcast clients can be triggered to flip into interleave mode.

201609130162

- Symptom: An MSR router reboots unexpectedly because of memory exhaustion.
- Condition: This symptom might occur if the router is enabled with SNMP and SNMP notifications and a user Telnets to the router by using a username longer than 253 bytes.

201609130139

- Symptom(1): CVE-2015-8138.
- Condition(1): To distinguish legitimate peer responses from forgeries, a client attempts to verify a response packet by ensuring that the origin timestamp in the packet matches the origin timestamp it transmitted in its last request. A logic error exists that allows packets with an origin timestamp of zero to bypass this check whenever there is not an outstanding request to the server.
- Symptom(2): CVE-2015-7979.
- Condition(2): An off-path attacker can send broadcast packets with bad authentication (wrong key, mismatched key, incorrect MAC, etc) to broadcast clients. It is observed that the broadcast client tears down the association with the broadcast server upon receiving just one bad packet.
- Symptom(3): CVE-2015-7974.
- Condition(3): Symmetric key encryption uses a shared trusted key. The reported title for this issue was "Missing key check allows impersonation between authenticated peers" and the

report claimed "A key specified only for one server should only work to authenticate that server, other trusted keys should be refused." Except there has never been any correlation between this trusted key and server v. clients machines and there has never been any way to specify a key only for one server. We have treated this as an enhancement request, and ntp-4.2.8p6 includes other checks and tests to strengthen clients against attacks coming from broadcast servers.

- Symptom(4): CVE-2015-7973.
- Condition(4): If an NTP network is configured for broadcast operations, then either a man-in-the-middle attacker or a malicious participant that has the same trusted keys as the victim can replay time packets.

201609130143

- Symptom(1): CVE-2016-1550
- Condition(1): Packet authentication tests have been performed using memcmp() or possibly bcmp(), and it is potentially possible for a local or perhaps LAN-based attacker to send a packet with an authentication payload and indirectly observe how much of the digest has matched.
- Symptom(2): CVE-2016-1551
- Condition(2): While the majority OSes implement martian packet filtering in their network stack, at least regarding 127.0.0.0/8, a rare few will allow packets claiming to be from 127.0.0.0/8 that arrive over physical network. On these OSes, if ntpd is configured to use a reference clock an attacker can inject packets over the network that look like they are coming from that reference clock.
- Symptom(3): CVE-2016-2519
- Condition(3): ntpq and ntpdc can be used to store and retrieve information in ntpd. It is possible to store a data value that is larger than the size of the buffer that the ctl_getitem() function of ntpd uses to report the return value. If the length of the requested data value returned by ctl_getitem() is too large, the value NULL is returned instead. There are 2 cases where the return value from ctl_getitem() was not directly checked to make sure it's not NULL, but there are subsequent INSIST() checks that make sure the return value is not NULL. There are no data values ordinarily stored in ntpd that would exceed this buffer length. But if one has permission to store values and one stores a value that is "too large", then ntpd will abort if an attempt is made to read that oversized value.
- Symptom(4): CVE-2016-1547
- Condition(4): For ntp-4 versions up to but not including ntp-4.2.8p7, an off-path attacker can cause a preemptable client association to be demobilized by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled.

  Furthermore, if the attacker keeps sending crypto NAK packets, for example one every second, the victim never has a chance to reestablish the association and synchronize time with that legitimate server.

  For ntp-4.2.8 thru ntp-4.2.8p6 there is less risk because more stringent checks are performed on incoming packets, but there are still ways to exploit this vulnerability in versions before ntp-4.2.8p7.
- Symptom(5): CVE-2016-1548
- Condition(5): It is possible to change the time of an ntpd client or deny service to an ntpd client by forcing it to change from basic client/server mode to interleaved symmetric mode. An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the client will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has been changed. Ntpq gives no indication that the mode has been switched.
- Symptom(6): CVE-2015-7704
- Condition(6): The fix for NtpBug2901 in ntp-4.2.8p4 went too far, breaking peer associations.

Resolved problems in CMW710-R0407

201604200673

- Symptom: A GE interface goes down after the speed auto 1000 command is executed on the interface.
- Condition: This symptom occurs if the speed auto 1000 command, which is not supported by a GE interface, is executed on a GE interface.

Resolved problems in CMW710-E0404P06

201602030095

- Symptom: The router displays incorrect output during a boot process.
- Condition: This symptom might occur if the router is powered on.

Resolved problems in CMW710-R0304P12

201508030418

- Symptom: The **reset counters interface** command cannot clear the rate statistics on Eth-channel interfaces.
- Condition: This symptom might occur if the **reset counters interface** command is used to clear the rate statistics on Eth-channel interfaces.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

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

  www.hpe.com/support/hpesc

Information to collect:

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

Documents

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

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

Related documents

The following documents provide related information:

- HPE FlexNetwork MSR954 Routers Quick Start
- HPE FlexNetwork MSR954 Routers Installation Guide
- HPE FlexNetwork MSR958 Routers Quick Start
- HPE FlexNetwork MSR958 Routers Installation Guide
- HPE FlexNetwork MSR Router Series Configuration Guides
- HPE FlexNetwork MSR Router Series Command References

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 MSR954P_MSR958 specifications

Item	JH300A	JH301A	JH373A
Console port	1		
USB port	1		
GE WAN port	1GE+1Combo	1GE+1Combo	1GE
GE LAN port	8	8	4
Memory	DDR III 1GB		
Flash	256MB		
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	330×230×44.2mm	330×230×44.2mm	300×200×44.2mm
AC power adapter	100V AC～240V AC，50Hz～60Hz		
Max. AC power	20W	20W+65W(PoE)	24W
Operating temperature	0℃～45℃	0℃～45℃	0℃～40℃
Relative humidity (non-condensing)	5%～90%		

Table 6 MSR954 specifications

Item	JH296A	JH297A	JH298A	JH299A
Console port	1			
USB port	2	2	1	1
GE WAN port	2			
GE LAN port	4			
Memory	DDR III 1GB			
Flash	256MB			
Dimensions (H × W × D) (excluding rubber feet and mounting brackets)	43.6 × 266 × 161 mm (1.72 × 10.47 × 6.34 in)			
AC power adapter	100V AC～240V AC，50Hz～60Hz			
Max. AC power	15W			
Operating temperature	0℃～45℃			
Relative humidity (non-condensing)	5%～90%			

Software features

Table 7 software features

Category	Features
LAN protocol:	ARP: proxy ARP, gratuitous ARP, and authorized ARP Ethernet_II Ethernet_SNAP VLAN: port-based VLAN and VLAN-based port isolation 802.3x 802.1p 802.1Q 802.1X STP, RSTP, and MSTP Port multicast suppression VXLAN
WAN protocols:	PPPoE client/server DCC 3G/4G
IP services	Fast forwarding (unicast or multicast) TCP UDP IP unnumbered Policy-based routing (unicast or multicast)
IP application	Ping and Trace DHCP server DHCP client DNS client DNS static DNS proxy DDNS NQA NTP Telnet TFTP client FTP client FTP server IPHC
IP route	Static routing Dynamic routing protocols: RIP, OSPF, BGP, and IS-IS Routing policy
AAA	Local authentication RADIUS HWTACACS LDAP

Firewall	ASPF ACL Filter Security zone-based firewall
Security	Port security IPsec Portal L2TP NAT and NAPT PKI RSA SSH v1.5 and SSH v2.0 uRPF GRE
Reliability	VRRP Interface backup BFD Load balancing Track
Traffic supervision	CAR (Committed Access Rate) LR (Line Rate)
Congestion management	FIFO, PQ, CQ, WFQ, CBQ, and RTPQ
Congestion avoidance	WRED/RED
Traffic shaping	GTS(Generic Traffic Shaping)
Other QOS technologies	IPHC Sub-interface QOS
Network management	SNMPv1, SNMPv2c, and SNMPv3 MIB Information center NETCONF SMS-based automatic configuration USB-based automatic configuration Web-based network management EAA
Local management	CLI-based network management License management File system management Automatic configuration Startup image backup
User access management	Console login TTY login Telnet login SSH login

	FTP access XMODEM access

Appendix B Upgrading software

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

Software types

The following software types are available:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load application software and the startup configuration file or manage files when the device cannot correctly start up.
- **Comware image**—Includes the following image subcategories:
  - **Boot image**—A .bin file that contains the Linux operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
  - **System image**—A .bin file that contains the minimum feature modules required for device operation and some basic features, including device management, interface management, configuration management, and routing. To have advanced features, you must purchase feature packages.
  - **Feature package**—Includes a set of advanced software features. Users purchase feature packages as needed.
  - **Patch packages**—Irregularly released packages for fixing bugs without rebooting the device. A patch package does not add new features or functions.

  Comware software images that have been loaded are called "current software images." Comware images specified to load at the next startup are called "startup software images."

Boot ROM image, boot image, and system image are required for the system to work. These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images and sets them as startup software images.

Upgrade methods

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

Upgrade method	Remarks
Centralized devices upgrading from the CLI	You must reboot the router to complete the upgrade. This method can interrupt ongoing network services.
Distributed devices upgrading from the CLI	You must reboot the router to complete the upgrade. This method can interrupt ongoing network services.
Distributed devices ISSU	This method upgrades the router with the least amount of downtime.
Managing files from the BootWare menu	Use this method when the router cannot correctly start up.

Preparing for the upgrade

Before you upgrade system software, complete the following tasks:

- Set up the upgrade environment as shown in Table 9.
- Configure routes to make sure that the router and the file server can reach each other.
- Run a TFTP or FTP server on the file server.
- Log in to the CLI of the router through the console port.
- Copy the upgrade file to the file server and correctly set the working directory on the TFTP or FTP server.
- Make sure the upgrade has minimal impact on the network services. During the upgrade, the router cannot provide any services.

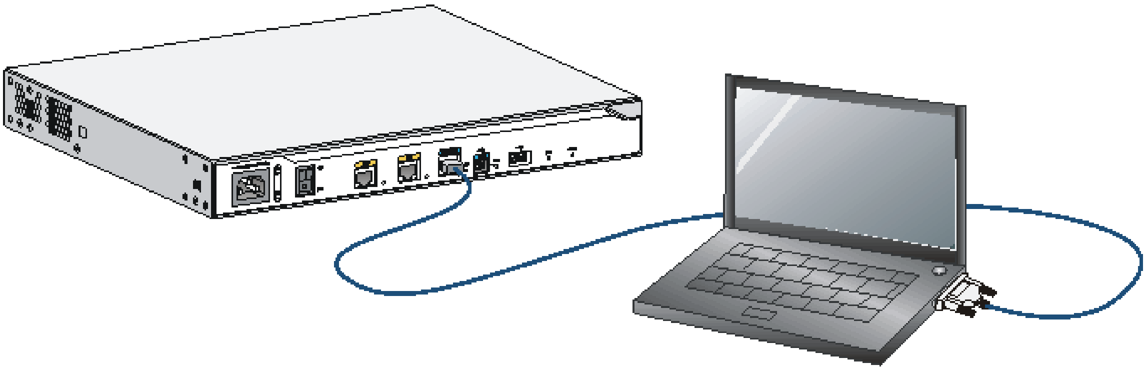
IMPORTANT:

In the BootWare menu, if you choose to download files over Ethernet, the Ethernet port must be GE0 on an MSR954P, MSR958, MSR2003, MSR2004-24, MSR2004-48, MSR3012, MSR3024, MSR3044, and MSR3064 router, and must be M-GE0 on an MSR4060 and MSR4080 router.

Table 8 Storage media

Model	Storage medium	Path	Router Types
MSR954P	Flash	flash:/	Centralized devices
MSR958	Flash	flash:/	Centralized devices
MSR2003	Flash	flash:/	Centralized devices
MSR2004-24	Flash	flash:/	Centralized devices
MSR2004-48	Flash	flash:/	Centralized devices
MSR3012	CF card	cfa0:/	Centralized devices
MSR3024	CF card	cfa0:/	Centralized devices
MSR3044	CF card	cfa0:/	Centralized devices
MSR3064	CF card	cfa0:/	Centralized devices
MSR4060	CF card	cfa0:/	Centralized devices
MSR4080	CF card	cfa0:/	Distributed devices

Figure 1 Set up the upgrade environment



Centralized devices upgrading 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.

Saving the running configuration and verifying the storage space

1. Save the running configuration

```
<HPE>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):
Validating file. Please wait...
Configuration is saved to device successfully.
<HPE>
```

2. Identify the system software image and configuration file names and verify that the flash has sufficient space for the new system software image.

```
<HPE>dir
Directory of flash:
   0 drw-           - Aug 15 2012 12:03:13   diagfile
   1 -rw-          84 Aug 15 2012 12:17:59   ifindex.dat
   2 drw-           - Aug 15 2012 12:03:14   license
   3 drw-           - Aug 15 2012 12:03:13   logfile
   4 -rw-    11418624 Dec 15 2011 09:00:00   msr2000-cmw710-boot-a0005.bin
   5 -rw-     1006592 Dec 15 2011 09:00:00   msr2000-cmw710-data-a0005.bin
   6 -rw-       10240 Dec 15 2011 09:00:00   msr2000-cmw710-security-a0005.bin
   7 -rw-    24067072 Dec 15 2011 09:00:00   msr2000-cmw710-system-a0005.bin
   8 -rw-     1180672 Dec 15 2011 09:00:00   msr2000-cmw710-voice-a0005.bin
   9 drw-           - Aug 15 2012 12:03:13   seclog
  10 -rw-        1632 Aug 15 2012 12:18:00   startup.cfg
  11 -rw-       25992 Aug 15 2012 12:18:00   startup.mdb

262144 KB total (223992 KB free)
```

```
<HPE>
```

Downloading the image file to the router

Using TFTP

Download the system software image file, for example, msr2000.ipe to the flash on the router.

```
<HPE>tftp 192.168.1.100 get msr2000.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 35.9M  100 35.9M    0     0   559k      0  0:01:05  0:01:05 --:--:--  546k

<HPE>
```

Using FTP

1. From FTP client view, download the system software image file (for example, msr26.ipe) to the CF card on the router.

```
ftp> get msr2000.ipe
msr2000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)

[ftp]
```

2. Return to user view.

```
[ftp]quit
221 Service closing control connection

 <HPE>
```

Specifying the startup image file

1. Specify the msr2000.ipe file as the main image file at the next reboot.

```
<HPE>boot-loader file flash:/msr2000.ipe main
Images in IPE:
  msr2000-cmw710-boot-a0005.bin
  msr2000-cmw710-system-a0005.bin
  msr2000-cmw710-security-a0005.bin
  msr2000-cmw710-voice-a0005.bin
  msr2000-cmw710-data-a0005.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to the device.
Successfully copied flash:/msr2000-cmw710-boot-a0005.bin to
flash:/msr2000-cmw710-boot-a0005.bin.

Successfully copied flash:/msr2000-cmw710-system-a0005.bin to
flash:/msr2000-cmw710-system-a0005.bin.
```

```
Successfully copied flash:/msr2000-cmw710-security-a0005.bin to
flash:/msr2000-cmw710-security-a0005.bin.

Successfully copied flash:/msr2000-cmw710-voice-a0005.bin to
flash:/msr2000-cmw710-voice-a0005.bin.

Successfully copied flash:/msr2000-cmw710-data-a0005.bin to
flash:/msr2000-cmw710-data-a0005.bin.

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

<HPE>
```

2. Verify that the file has been loaded.

```
<HPE> display boot-loader
Software images on the device:
Current software images:
  flash:/msr2000-cmw710-boot-a0004.bin
  flash:/msr2000-cmw710-system-a0004.bin
  flash:/msr2000-cmw710-security-a0004.bin
  flash:/msr2000-cmw710-voice-a0004.bin
  flash:/msr2000-cmw710-data-a0004.bin
Main startup software images:
  flash:/msr2000-cmw710-boot-a0005.bin
  flash:/msr2000-cmw710-system-a0005.bin
  flash:/msr2000-cmw710-security-a0005.bin
  flash:/msr2000-cmw710-voice-a0005.bin
  flash:/msr2000-cmw710-data-a0005.bin
Backup startup software images:
  None
<HPE>
```

Rebooting and completing the upgrade

1. Reboot the router.

```
<HPE>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...
<HPE>
System is starting...
```

2. After the reboot is complete, verify that the system software image is correct.

```
<HPE> display version
HPE Comware Software, Version 7.1.042, Release 000702
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
HPE MSR2003 uptime is 0 weeks, 0 days, 13 hours, 23 minutes                    Last
reboot reason : User reboot
Boot image: flash:/msr2000-cmw710-boot-a0005.bin
Boot image version: 7.1.040, Alpha 0005
System image: flash:/msr2000-cmw710-system-a0005.bin
System image version: 7.1.040, Alpha 0005

CPU ID: 0x1
1G bytes DDR3 SDRAM Memory
2M bytes Flash Memory
PCB               Version:  3.0
CPLD              Version:  1.0
Basic    BootWare Version:  1.04
Extended BootWare Version:  1.04
[SLOT  0]AUX                        (Hardware)3.0    (Driver)1.0,   (Cpld)1.0
[SLOT  0]GE0/0                      (Hardware)3.0    (Driver)1.0,   (Cpld)1.0
[SLOT  0]GE0/1                      (Hardware)3.0    (Driver)1.0,   (Cpld)1.0
[SLOT  0]CELLULAR0/0                (Hardware)3.0    (Driver)1.0,   (Cpld)1.0

<HPE>
```

Distributed devices upgrading 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.

Display the slot number of the active MPU

Perform the **display device** command in any view to display the slot number of the active MPU. By default, the standby MPU will automatically synchronize the image files from active MPU.

```
<HPE>display device
 Slot No.      Board Type                Status        Primary        SubSlots
 ---------------------------------------------------------------------------
 0             MPU-100                   Normal        Master           0
 1             MPU-100                   Normal        Standby          0
 2             SPU-100                   Normal        N/A              10
<HPE>
```

Save the current configuration and verify the storge space

1. Perform the **save** command in any view to save the current configuration.

```
<HPE>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Configuration is saved to device successfully.
<HPE>
```

2. Perform the **dir** command in user view to identify the system software image and configuration file names and verify that the CF card has sufficient space for the new system software image.

```
<HPE>dir
Directory of cfa0:
   0 drw-           - Jan 07 2013 14:02:12   diagfile
   1 -rw-         307 Jan 22 2013 17:02:02   ifindex.dat
   2 drw-           - Jan 07 2013 14:02:12   license
   3 drw-           - Jan 22 2013 13:42:00   logfile
   4 -rw-    21412864 Jan 22 2013 16:49:00   MSR4000-cmw710-boot-r0005p01.bin
   5 -rw-     1123328 Jan 22 2013 16:50:30   MSR4000-cmw710-data-r0005p01.bin
   6 -rw-       11264 Jan 22 2013 16:50:26   MSR4000-cmw710-security-r0005p01.bin
   7 -rw-    45056000 Jan 22 2013 16:49:34   MSR4000-cmw710-system-r0005p01.bin
   8 -rw-     2746368 Jan 22 2013 16:50:26   MSR4000-cmw710-voice-r0005p01.bin
   9 drw-           - Jan 07 2013 14:02:12   seclog
  10 -rw-        2166 Jan 22 2013 17:02:02   startup.cfg
  11 -rw-       34425 Jan 22 2013 17:02:02   startup.mdb

507492 KB total (438688 KB free)

<HPE>
```

Download the image file to the router

Using TFTP

Perform the **tftp get** command in user view to download the system software image file, for example, msr4000.ipe to the CF card on the router.

```
<HPE>tftp 192.168.1.100 get msr4000.ipe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total     Spent    Left  Speed
 45 67.0M   45 30.4M    0     0   792k      0  0:01:26  0:00:39  0:00:47  844k
100 67.0M  100 67.0M    0     0   772k      0  0:01:28  0:01:28 --:--:--  745k
<HPE>
```

Using FTP

1. Perform the **get** command in FTP client view to download the system software image file msr4000.ipe to the CF card on the router.

```
ftp> get msr4000.ipe
msr4000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)
[ftp]
```

2. Perform the **quit** command in FTP client view to return to user view.

```
[ftp]quit
221 Service closing control connection
 <HPE>
```

Copy the image file to CF card root directory of the standby MPU

```
<HPE> copy msr4000.ipe slot1#cfa0:/
Copy cfa0:/msr4000.ipe to slot1#cfa0:/msr4000.ipe?[Y/N]:y
Copying file cfa0:/msr4000.ipe to slot1#cfa0:/ msr4000.ipe...Done.
```

Specifying the startup image file

1. Perform the **boot-loader** command in user view to d specify the msr4000.ipe file as the main image file for the active MPU on slot 0 at the next reboot.

```
<HPE>boot-loader file flash:/msr4000.ipe slot 0 main
Images in IPE:
  msr4000-cmw710-boot-a0005.bin
  msr4000-cmw710-system-a0005.bin
  msr4000-cmw710-security-a0005.bin
  msr4000-cmw710-voice-a0005.bin
  msr4000-cmw710-data-a0005.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to the device.
Successfully copied flash:/msr4000-cmw710-boot-a0005.bin to
cfa0:/msr4000-cmw710-boot-a0005.bin.
Successfully copied flash:/msr4000-cmw710-system-a0005.bin to
cfa0:/msr4000-cmw710-system-a0005.bin.
Successfully copied flash:/msr4000-cmw710-security-a0005.bin to
cfa0:/msr4000-cmw710-security-a0005.bin.
Successfully copied flash:/msr4000-cmw710-voice-a0005.bin to
cfa0:/msr4000-cmw710-voice-a0005.bin.
Successfully copied flash:/msr4000-cmw710-data-a0005.bin to
cfa0:/msr4000-cmw710-data-a0005.bin.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on the device.
<HPE>
```

2. Perform the **boot-loader** command in user view to d specify the msr4000.ipe file as the main image file for the standby MPU on slot 1 at the next reboot.

```
<HPE>boot-loader file flash:/msr4000.ipe slot 0 main
Images in IPE:
  msr4000-cmw710-boot-a0005.bin
  msr4000-cmw710-system-a0005.bin
  msr4000-cmw710-security-a0005.bin
  msr4000-cmw710-voice-a0005.bin
  msr4000-cmw710-data-a0005.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to the device.
Successfully copied flash:/msr4000-cmw710-boot-a0005.bin to
cfa0:/msr4000-cmw710-boot-a0005.bin.
Successfully copied flash:/msr4000-cmw710-system-a0005.bin to
cfa0:/msr4000-cmw710-system-a0005.bin.
Successfully copied flash:/msr4000-cmw710-security-a0005.bin to
cfa0:/msr4000-cmw710-security-a0005.bin.
Successfully copied flash:/msr4000-cmw710-voice-a0005.bin to
cfa0:/msr4000-cmw710-voice-a0005.bin.
Successfully copied flash:/msr4000-cmw710-data-a0005.bin to
cfa0:/msr4000-cmw710-data-a0005.bin.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on the device.
<HPE>
```

3. Perform the **display boot-loader** command in user view to verify that the file has been loaded.

```
<HPE> display boot-loader
Software images on slot 0:
Current software images:
  cfa0:/MSR4000-cmw710-boot-a0004.bin
  cfa0:/MSR4000-cmw710-system-a0004.bin
  cfa0:/MSR4000-cmw710-security-a0004.bin
  cfa0:/MSR4000-cmw710-voice-a0004.bin
  cfa0:/MSR4000-cmw710-data-a0004.bin
Main startup software images:
  cfa0:/MSR4000-cmw710-boot-a0005.bin
  cfa0:/MSR4000-cmw710-system-a0005.bin
  cfa0:/MSR4000-cmw710-security-a0005.bin
  cfa0:/MSR4000-cmw710-voice-a0005.bin
  cfa0:/MSR4000-cmw710-data-a0005.bin
Backup startup software images:
  None
Software images on slot 1:
Current software images:
  cfa0:/MSR4000-cmw710-boot-r0005p01.bin
  cfa0:/MSR4000-cmw710-system-r0005p01.bin
  cfa0:/MSR4000-cmw710-security-r0005p01.bin
  cfa0:/MSR4000-cmw710-voice-r0005p01.bin
  cfa0:/MSR4000-cmw710-data-r0005p01.bin
Main startup software images:
  cfa0:/MSR4000-cmw710-boot-r0005p01.bin
  cfa0:/MSR4000-cmw710-system-r0005p01.bin
  cfa0:/MSR4000-cmw710-security-r0005p01.bin
  cfa0:/MSR4000-cmw710-voice-r0005p01.bin
  cfa0:/MSR4000-cmw710-data-r0005p01.bin
Backup startup software images:
  None
```

Reboot and completing the upgrade

1. Perform the **reboot** command in user view to reboot the router.

```
<HPE>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...
<HPE>
System is starting..
```

2. After the reboot is complete, perform the **display version** command to verify that the system software image is correct.

```
<HPE> display version
HPE Comware Software, Version 7.1.042, Release 000702
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
HPE MSR4060 uptime is 0 weeks, 0 days, 11 hours, 49 minutes
```

```
Last reboot reason : Power on
Boot image: cfa0:/MSR4000-cmw710-boot-a0005.bin
Boot image version: 7.1.040, Alpha 0005
System image: cfa0:/MSR4000-cmw710-system-a0005.bin
System image version: 7.1.040, Alpha 0005
Feature image(s) list:
  cfa0:/MSR4000-cmw710-security-a0005.bin, version: 7.1.040
  cfa0:/MSR4000-cmw710-voice-a0005.bin, version: 7.1.040
  cfa0:/MSR4000-cmw710-data-a0005.bin, version: 7.1.040

Slot 0: MPU-100 uptime is 0 week, 0 day, 1 hour, 20 minutes
Last reboot reason : Power on
CPU ID: 0x3
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB               Version:  2.0
CPLD              Version:  1.0
Basic    BootWare Version:  1.04
Extended BootWare Version:  1.04
[SUBSLOT  0]CON                    (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]AUX                    (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]MGE0                   (Hardware)2.0    (Driver)1.0,   (Cpld)1.0

Slot 1: MPU-100 uptime is 0 week, 0 day, 1 hour, 8 minutes
Last reboot reason : User reboot
CPU ID: 0x3
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB               Version:  2.0
CPLD              Version:  1.0
Basic    BootWare Version:  1.05
Extended BootWare Version:  1.05
[SUBSLOT  0]CON                    (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]AUX                    (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]MGE0                   (Hardware)2.0    (Driver)1.0,   (Cpld)1.0

Slot 2: SPU-100 uptime is 0 week, 0 day, 1 hour, 19 minutes
Last reboot reason : Power on
CPU ID: 0x5
2G bytes DDR3 SDRAM Memory
8M bytes Flash Memory
PCB               Version:  2.0
CPLD              Version:  1.0
Basic    BootWare Version:  1.02
Extended BootWare Version:  1.02
[SUBSLOT  0]GE2/0/0                (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]GE2/0/1                (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]GE2/0/2                (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
```

```
[SUBSLOT  0]GE2/0/3               (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]CELLULAR2/0/0         (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  0]CELLULAR2/0/1         (Hardware)2.0    (Driver)1.0,   (Cpld)1.0
[SUBSLOT  1]HMIM-4SAE             (Hardware)3.0    (Driver)1.0,   (Cpld)4.0
```

Distributed devices ISSU

The In-Service Software Upgrade (ISSU) function enables software upgrade with the least amount of downtime.

To implement ISSU of a distributed device, use these guidelines:

- Make sure the device has two MPUs.
- Upgrade the standby MPU is upgraded first to form a new forwarding plane and a new control plane.
- Upgrade the active MPU after the standby MPU operates correctly. The standby MPU will synchronize data and configuration from the active MPU and take over the forwarding and control functions.

Disabling the standby MPU auto-update function

When you upgrade the active MPU of a dual-MPU distributed device, the standby MPU auto-update function automatically upgrades the standby MPU by default. To use ISSU, you must disable the function.

To disable the standby MPU auto-update function:

1. View the roles of the MPUs.

```
<HPE>display device
 Slot No.      Board Type                Status        Primary        SubSlots
 -----------------------------------------------------------------------------
 0             MPU-100                   Normal        Master             0
 1             MPU-100                   Normal        Standby            0
 2             SPU-100                   Normal        N/A                10
<HPE>
```

   The output shows that the MPU in slot 0 is the active MPU.

2. Disable the standby MPU auto-update function.

```
<HPE>system-view
[Sysname]version check ignore
[Sysname]undo version auto-update enable
```

Saving the running configuration and verifying the storage space

1. Save the running configuration.

```
<HPE>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Configuration is saved to device successfully.
```

```
<HPE>
```

2. Check the storage space.

```
<HPE>dir
Directory of cfa0:
   0 drw-           - Jan 07 2014 14:02:12   diagfile
   1 -rw-         307 Jan 22 2014 17:02:02   ifindex.dat
   2 drw-           - Jan 07 2014 14:02:12   license
   3 drw-           - Jan 22 2014 13:42:00   logfile
   4 -rw-    20050944 Jan 10 2014 09:06:48   msr4000-cmw710-boot-e010204.bin
   5 -rw-     2001920 Jan 10 2014 09:08:28   msr4000-cmw710-data-e010204.bin
   6 -rw-       11264 Jan 10 2014 09:08:18   msr4000-cmw710-security-e010204.bin
   7 -rw-    61538304 Jan 10 2014 09:07:36   msr4000-cmw710-system-e010204.bin
   8 -rw-     3232768 Jan 10 2014 09:08:22   msr4000-cmw710-voice-e010204.bin
   9 drw-           - Jan 07 2014 14:02:12   seclog
   10 -rw-       2166 Jan 22 2014 17:02:02   startup.cfg
   11 -rw-      34425 Jan 22 2014 17:02:02   startup.mdb

507492 KB total (438688 KB free)

<HPE>
```

The output shows the CF card has 438688 KB of free storage space. If the CF card of your device is not sufficient for the upgrade image, delete unused files.

Downloading the upgrade image file to the router

Using TFTP

Download the upgrade image file (for example, msr4000.ipe) to the CF card on the router.

```
<HPE>tftp 192.168.1.100 get msr4000.ipe
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 45 67.0M   45 30.4M    0     0   792k      0  0:01:26  0:00:39  0:00:47  844k
100 67.0M  100 67.0M    0     0   772k      0  0:01:28  0:01:28 --:--:--  745k
<HPE>
```

Using FTP

1. From FTP client view, download the upgrade image file (for example, msr4000.ipe) to the CF card on the router.

```
ftp> get msr4000.ipe
msr4000.ipe already exists. Overwrite it? [Y/N]:y
227 Entering passive mode (192,168,1,100,5,20)
125 Using existing data connection
226 Closing data connection; File transfer successful.
37691392 bytes received in 17.7 seconds (2.03 Mbyte/s)
[ftp]
```

2. Return to user view.

```
[ftp]quit
221 Service closing control connection
<HPE>
```

Copying the image file to the root directory of the CF card on the standby MPU

```
<HPE> copy msr4000.ipe slot1#cfa0:/
Copy cfa0:/msr4000.ipe to slot1#cfa0:/msr4000.ipe?[Y/N]:y
Copying file cfa0:/msr4000.ipe to slot1#cfa0:/ msr4000.ipe...Done.
```

Upgrading the standby MPU

1. Specify the msr4000.ipe file as the main startup image file for the standby MPU.

```
<HPE>boot-loader file msr4000.ipe slot 1 main
Verifying the IPE file and the images......Done.
HPE MSR4060 images in IPE:
  msr4000-cmw710-boot-e010305.bin
  msr4000-cmw710-system-e010305.bin
  msr4000-cmw710-security-e010305.bin
  msr4000-cmw710-voice-e010305.bin
  msr4000-cmw710-data-e010305.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
Decompressing file msr4000-cmw710-boot-e010305.bin to
slot1#cfa0:/msr4000-cmw710-boo
t-e010305.bin..............Done.
Decompressing file msr4000-cmw710-system-e010305.bin to
slot1#cfa0:/msr4000-cmw710-s
ystem-e010305.bin...............................................Done.
Decompressing file msr4000-cmw710-security-e010305.bin to
slot1#cfa0:/msr4000-cmw710
-security-e010305.bin...Done.
Decompressing file msr4000-cmw710-voice-e010305.bin to
slot1#cfa0:/msr4000-cmw710-vo
ice-e010305.bin....Done.
Decompressing file msr4000-cmw710-data-e010305.bin to
slot1#cfa0:/msr4000-cmw710-dat
a-e010305.bin...Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 1.
```

2. Reboot the standby MPU.

```
<HPE>reboot slot 1
This command will reboot the specified slot, Continue? [Y/N]:y
Now rebooting, please wait...
```

3. After the standby MPU starts up, verify the startup image files.

```
<HPE>display boot-loader
Software images on slot 0:
Current software images:
  cfa0:/msr4000-cmw710-boot-e010204.bin
  cfa0:/msr4000-cmw710-system-e010204.bin
  cfa0:/msr4000-cmw710-security-e010204.bin
  cfa0:/msr4000-cmw710-voice-e010204.bin
  cfa0:/msr4000-cmw710-data-e010204.bin
Main startup software images:
  cfa0:/msr4000-cmw710-boot-e010204.bin
  cfa0:/msr4000-cmw710-system-e010204.bin
  cfa0:/msr4000-cmw710-security-e010204.bin
  cfa0:/msr4000-cmw710-voice-e010204.bin
  cfa0:/msr4000-cmw710-data-e010204.bin
Backup startup software images:
  cfa0:/msr4000-cmw710-boot-e010203.bin
  cfa0:/msr4000-cmw710-system-e010203.bin
  cfa0:/msr4000-cmw710-security-e010203.bin
  cfa0:/msr4000-cmw710-voice-e010203.bin
  cfa0:/msr4000-cmw710-data-e010203.bin
Software images on slot 1:
Current software images:
  cfa0:/msr4000-cmw710-boot-e010305.bin
  cfa0:/msr4000-cmw710-system-e010305.bin
  cfa0:/msr4000-cmw710-security-e010305.bin
  cfa0:/msr4000-cmw710-voice-e010305.bin
  cfa0:/msr4000-cmw710-data-e010305.bin
Main startup software images:
  cfa0:/msr4000-cmw710-boot-e010305.bin
  cfa0:/msr4000-cmw710-system-e010305.bin
  cfa0:/msr4000-cmw710-security-e010305.bin
  cfa0:/msr4000-cmw710-voice-e010305.bin
  cfa0:/msr4000-cmw710-data-e010305.bin
Backup startup software images:
  cfa0:/msr4000-cmw710-boot-e010203.bin
  cfa0:/msr4000-cmw710-system-e010203.bin
  cfa0:/msr4000-cmw710-security-e010203.bin
  cfa0:/msr4000-cmw710-voice-e010203.bin
  cfa0:/msr4000-cmw710-data-e010203.bin
```

The output shows that the standby MPU is running the new images.

Upgrading the active MPU

1. Specify the msr4000.ipe file as the main startup image file for the active MPU.

```
<HPE>boot-loader file msr4000.ipe slot 0 main
Verifying the IPE file and the images......Done.
HPE MSR4060 images in IPE:
  msr4000-cmw710-boot-e010305.bin
  msr4000-cmw710-system-e010305.bin
  msr4000-cmw710-security-e010305.bin
  msr4000-cmw710-voice-e010305.bin
  msr4000-cmw710-data-e010305.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 0.
Decompressing file msr4000-cmw710-boot-e010305.bin to
cfa0:/msr4000-cmw710-boot-e010
305.bin..............Done.
```

```
Decompressing file msr4000-cmw710-system-e010305.bin to
cfa0:/msr4000-cmw710-system-
e010305.bin.............................................Done.
Decompressing file msr4000-cmw710-security-e010305.bin to
cfa0:/msr4000-cmw710-secur
ity-e010305.bin...Done.
Decompressing file msr4000-cmw710-voice-e010305.bin to
cfa0:/msr4000-cmw710-voice-e0
10305.bin....Done.
Decompressing file msr4000-cmw710-data-e010305.bin to
cfa0:/msr4000-cmw710-data-e010
305.bin...Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 0.
```

2. Reboot the active MPU.

```
<HPE>reboot slot 0
This command will reboot the specified slot, Continue? [Y/N]:y
Now rebooting, please wait...
```

The standby MPU takes over the forwarding and controlling functions before the active MPU reboots.

3. After the active MPU starts up, verify the startup image files.

```
<HPE>display boot-loader
Software images on slot 0:
Current software images:
  cfa0:/msr4000-cmw710-boot-e010305.bin
  cfa0:/msr4000-cmw710-system-e010305.bin
  cfa0:/msr4000-cmw710-security-e010305.bin
  cfa0:/msr4000-cmw710-voice-e010305.bin
  cfa0:/msr4000-cmw710-data-e010305.bin
Main startup software images:
  cfa0:/msr4000-cmw710-boot-e010305.bin
  cfa0:/msr4000-cmw710-system-e010305.bin
  cfa0:/msr4000-cmw710-security-e010305.bin
  cfa0:/msr4000-cmw710-voice-e010305.bin
  cfa0:/msr4000-cmw710-data-e010305.bin
Backup startup software images:
  cfa0:/msr4000-cmw710-boot-e010203.bin
  cfa0:/msr4000-cmw710-system-e010203.bin
  cfa0:/msr4000-cmw710-security-e010203.bin
  cfa0:/msr4000-cmw710-voice-e010203.bin
  cfa0:/msr4000-cmw710-data-e010203.bin
Software images on slot 1:
Current software images:
  cfa0:/msr4000-cmw710-boot-e010305.bin
  cfa0:/msr4000-cmw710-system-e010305.bin
  cfa0:/msr4000-cmw710-security-e010305.bin
  cfa0:/msr4000-cmw710-voice-e010305.bin
  cfa0:/msr4000-cmw710-data-e010305.bin
Main startup software images:
  cfa0:/msr4000-cmw710-boot-e010305.bin
  cfa0:/msr4000-cmw710-system-e010305.bin
  cfa0:/msr4000-cmw710-security-e010305.bin
  cfa0:/msr4000-cmw710-voice-e010305.bin
  cfa0:/msr4000-cmw710-data-e010305.bin
Backup startup software images:
  cfa0:/msr4000-cmw710-boot-e010203.bin
  cfa0:/msr4000-cmw710-system-e010203.bin
  cfa0:/msr4000-cmw710-security-e010203.bin
  cfa0:/msr4000-cmw710-voice-e010203.bin
  cfa0:/msr4000-cmw710-data-e010203.bin
```

4. Perform the **display boot-loader** command in user view to verify that the file has been loaded.

```
<HPE> display boot-loader
Software images on slot 0:
Current software images:
  cfa0:/MSR4000-cmw710-boot-r0005p01.bin
  cfa0:/MSR4000-cmw710-system-r0005p01.bin
  cfa0:/MSR4000-cmw710-security-r0005p01.bin
  cfa0:/MSR4000-cmw710-voice-r0005p01.bin
  cfa0:/MSR4000-cmw710-data-r0005p01.bin
Main startup software images:
  cfa0:/MSR4000-cmw710-boot-a0005.bin
  cfa0:/MSR4000-cmw710-system-a0005.bin
  cfa0:/MSR4000-cmw710-security-a0005.bin
  cfa0:/MSR4000-cmw710-voice-a0005.bin
  cfa0:/MSR4000-cmw710-data-a0005.bin
Backup startup software images:
  None
Software images on slot 1:
Current software images:
  cfa0:/MSR4000-cmw710-boot-r0005p01.bin
  cfa0:/MSR4000-cmw710-system-r0005p01.bin
  cfa0:/MSR4000-cmw710-security-r0005p01.bin
  cfa0:/MSR4000-cmw710-voice-r0005p01.bin
  cfa0:/MSR4000-cmw710-data-r0005p01.bin
Main startup software images:
  cfa0:/MSR4000-cmw710-boot-r0005p01.bin
  cfa0:/MSR4000-cmw710-system-r0005p01.bin
  cfa0:/MSR4000-cmw710-security-r0005p01.bin
  cfa0:/MSR4000-cmw710-voice-r0005p01.bin
  cfa0:/MSR4000-cmw710-data-r0005p01.bin
Backup startup software images:
  None
```

Upgrading from the BootWare menu

You can use the following methods to upgrade software from the BootWare menu:

- Using TFTP/FTP to upgrade software through an Ethernet port

- Using XMODEM to upgrade software through the console port

Accessing the BootWare menu

1. Power on the router (for example, an H3C MSR 2003 router), and you can see the following information:

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

****************************************************************************
*                                                                          *
*                    HPE MSR2003 BootWare, Version 1.20                     *
*                                                                          *
****************************************************************************
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.

Compiled Date       : Jun 22 2013
CPU ID              : 0x1
Memory Type         : DDR3 SDRAM
Memory Size         : 1024MB
Flash Size          : 2MB
Nand Flash size     : 256MB
CPLD Version        : 2.0
PCB Version         : 3.0


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

2. Press **Ctrl** + **B** to access the BootWare menu.

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

===========================<EXTEND-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
Enter your choice(0-9):
```

Table 9 BootWare menu options

Item	Description
<1> Boot System	Boot the system software image.
<2> Enter Serial SubMenu	Access the Serial submenu (see Table 12) for upgrading system software through the console port or changing the serial port settings.
<3> Enter Ethernet SubMenu	Access the Ethernet submenu (see Table 10) 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	Delete the next-startup configuration files and load the factory-default configuration.
<6> Skip Current System Configuration	Start the router with the factory default configuration. This is a one-time operation and does not take effect at the next reboot. You use this option when you forget the console login password.
<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. HPE does not recommend upgrading BootWare separately. This document does not cover using the BootWare Operation menu.
<8> Skip authentication for console login	Clear all the authentication schemes on the console port.
<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 software through an Ethernet port

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

```
===============================<File CONTROL>===============================
 |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                                                      |
============================================================================
Enter your choice(0-4):
```

Table 10 Ethernet submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download a system software image to the SDRAM and run the image.
<2> Update Main Image File	Upgrade the main system software image.
<3> Update Backup Image File	Upgrade the backup system software image.
<4> Download Files(*.*)	Download a system software image to the Flash or CF card.
<5> Modify Ethernet Parameter	Modify network settings.
<0> Exit To Main Menu	Return to the 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         :msr2000.ipe
                       :
Target File Name       :msr2000.ipe
                       :
Server IP Address      :192.168.1.1
Local IP Address       :192.168.1.100
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
FTP User Name          :user001
FTP User Password      :********
```

Table 11 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	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file 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. If a mask must be set, use a colon (:) to separate the mask length from the IP address. For example, 192.168.80.10:24.
Local IP Address	Set the IP address of the router.
Subnet Mask	Subnet Mask of the local IP address.
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. Select an option in the Ethernet submenu to upgrade a system software image. For example, enter **2** to upgrade the main system software image.

```
Loading.....................................................................
............................................................................
............................................................................
.........................................Done.
37691392 bytes downloaded!
The file is exist,will you overwrite it? [Y/N]Y
Image file msr2000-cmw710-boot-a0005.bin is self-decompressing...
Saving file flash:/msr2000-cmw710-boot-a0005.bin .............................
......Done.
Image file msr2000-cmw710-system-a0005.bin is self-decompressing...
Saving file flash:/msr2000-cmw710-system-a0005.bin ...........................
.........................................Done.
Image file msr2000-cmw710-security-a0005.bin is self-decompressing...
Saving file flash:/msr2000-cmw710-security-a0005.bin Done.
Image file msr2000-cmw710-voice-a0005.bin is self-decompressing...
Saving file flash:/msr2000-cmw710-voice-a0005.bin ......Done.
Image file msr2000-cmw710-data-a0005.bin is self-decompressing...
Saving file flash:/msr2000-cmw710-data-a0005.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(0-4):
```

4. Enter **0** to return to the BootWare menu

```
===========================<EXTEND-BOOTWARE MENU>===========================
|<1> Boot System                                                           |
|<2> Enter Serial SubMenu                                                  |
|<3> Enter Ethernet SubMenu                                                |
|<4> File Control                                                          |
|<5> Modify BootWare Password                                              |
|<6> Skip Current System Configuration                                     |
|<7> BootWare Operation Menu                                               |
|<8> Skip authentication for console login                                 |
|<9> Storage Device Operation                                              |
|<0> Reboot                                                                |
============================================================================
Enter your choice(0-9):
```

5. **1** to boot the system.

```
Loading the main image files...
Loading file flash:/msr2000-cmw710-system-a0005.bin.........................
Done.
Loading file flash:/msr2000-cmw710-boot-a0005.bin.............Done.

Image file flash:/msr2000-cmw710-boot-a0005.bin is self-decompressing.........
.....Done.
System image is starting...
Line aux0 is available.


Press ENTER to get started.
```

Using XMODEM to upgrade software through the console port

1. Enter **2** in the 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(0-4):
```

Table 12 Serial submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download an application to SDRAM through the serial port and run the program.
<2> Update Main Image File	Upgrade the main system software image.
<3> Update Backup Image File	Upgrade the backup system software image.
<4>Download Files(*.*)	Download a system software image to the Flash or CF card.
<5> Modify Serial Interface Parameter	Modify serial port parameters
<0> Exit To Main Menu	Return to the BootWare menu.

2. 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):
```

The following messages appear:

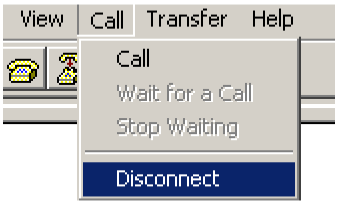
```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

NOTE:

Typically the size of a .bin file is over 10 MB. Even at 115200 bps, the download takes about 30 minutes.

3. Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the router.

Figure 2 Disconnect the terminal connection

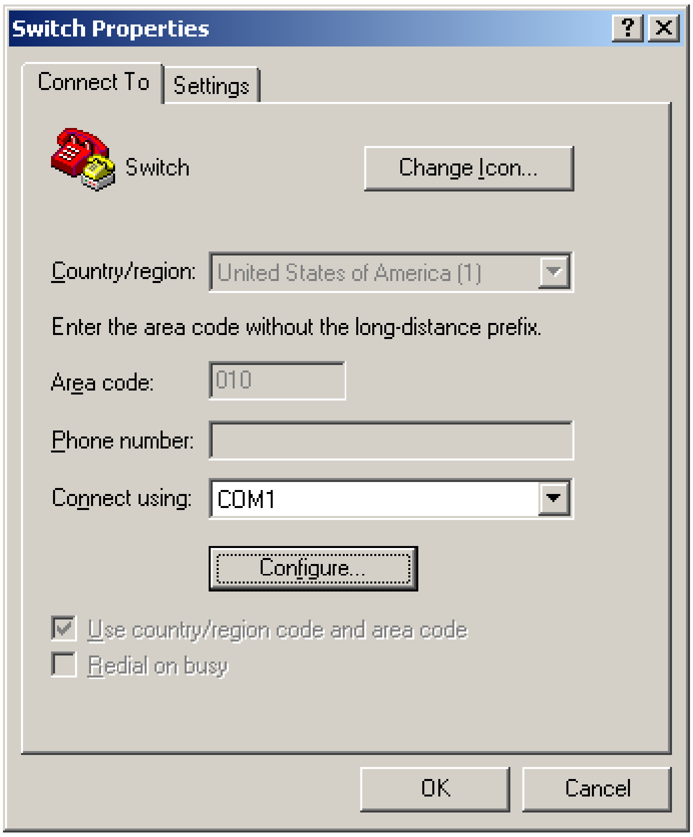


NOTE:

If the baud rate of the console port is 9600 bps, jump to step 9.

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

Figure 3 Properties dialog box



Switch Properties

Connect To | Settings

Switch

Country/region: United States of America (1)

Enter the area code without the long-distance prefix.

Area code: 010

Phone number:

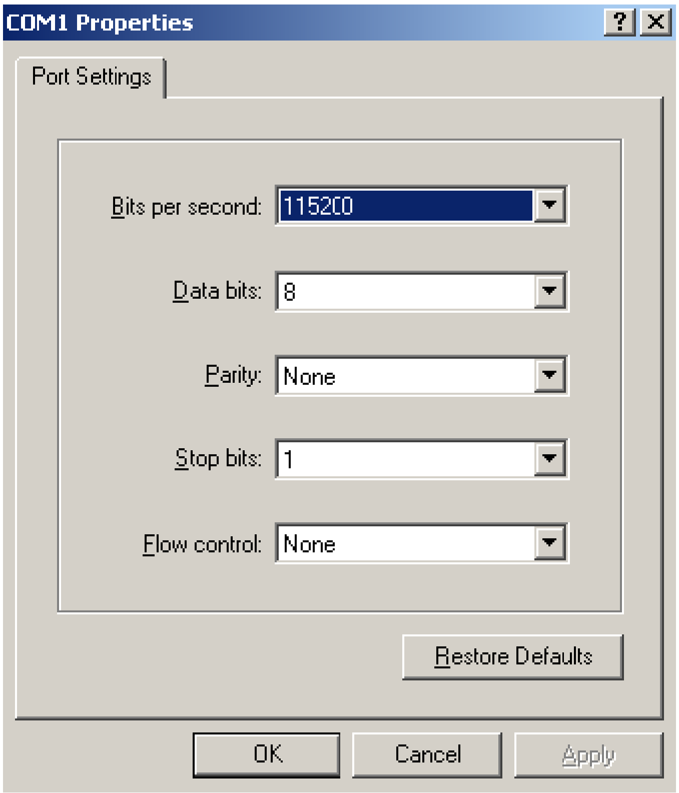
Connect using: COM1

☑ Use country/region code and area code

□ Redial on busy

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

Figure 4 Modify the baud rate



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

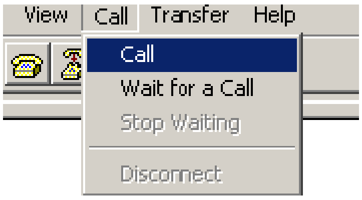
Parity: None

Stop bits: 1

Flow control: None

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

Figure 5 Reestablish the connection



7. Press **Enter.**

The following menu appears:

```
The current baudrate is 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):
```

8. Enter **0** to return to the Serial submenu.

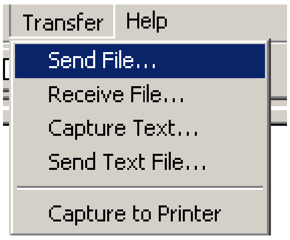
```
===========================<Enter Serial SubMenu>===========================
|Note:the operating device is flash                                        |
|<1> Download Image Program To SDRAM And Run                               |
|<2> Update Main Image File                                      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

9. Select an option from options **2** to **3** to upgrade a system software image. For example, enter **2** to upgrade the main system software image.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

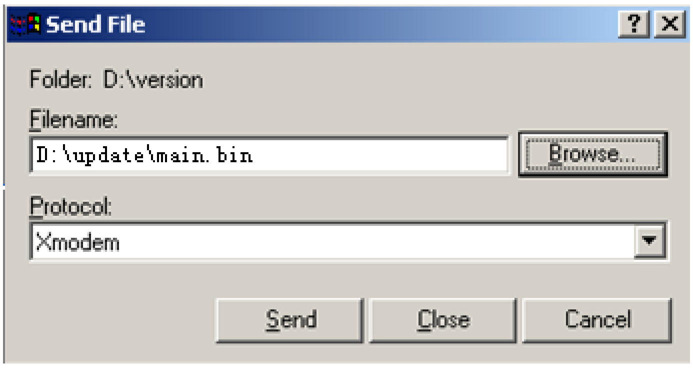
10. Select **Transfer** > **Send File** in the HyperTerminal window.

Figure 6 Transfer menu



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

Figure 7 File transmission dialog box


Send File

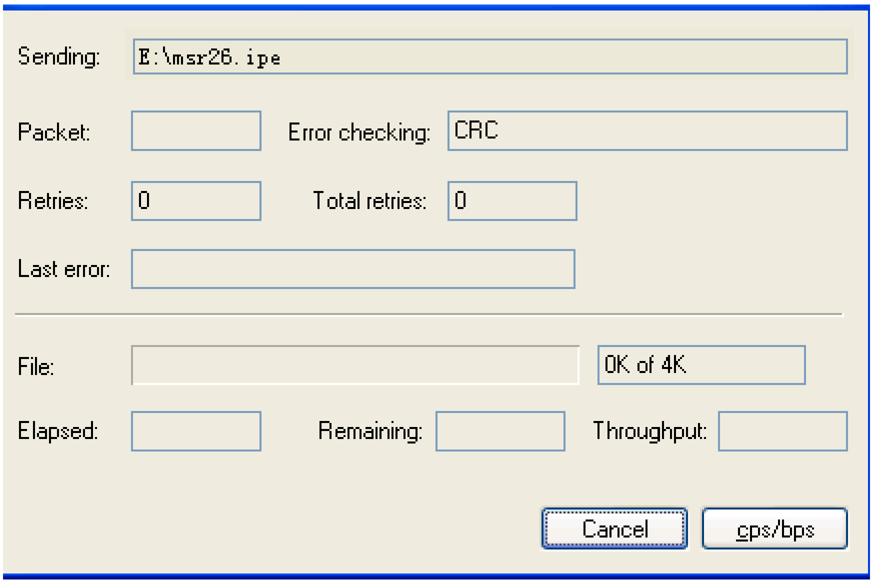
Folder: D:\version

Filename:
D:\update\main.bin

Protocol:
Xmodem

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

Figure 8 File transfer progress



Sending: E:\msr26.ipe

Packet: Error checking: CRC

Retries: 0 Total retries: 0

Last error:

File: 0K of 4K

Elapsed: Remaining: Throughput:

13. When the Serial submenu appears after the file transfer is complete, enter **0** at the prompt to return to the BootWare menu.

```
Download successfully!
37691392 bytes downloaded!
Input the File Name:main.bin
Updating File flash:/main.bin.............................................
.....................................................Done!

==========================<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(0-4):
```

14. Enter **1** in the BootWare menu to boot the system.
15. If you are using a download rate other than 9600 bps, change the baud rate of the terminal to 9600 bps. If the baud rate has been set to 9600 bps, skip this step.

Managing files from the BootWare menu

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

The File Control submenu appears:

```
============================<File CONTROL>=============================
|Note:the operating device is cfa0                                     |
|<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	Change the type of a system software image (.ipe).
<3> Set Bin File type	Change the type of a system software image (.bin).
<4> Set Configuration File type	Change the type of a configuration file.
<5> Delete File	Delete files.
<6> Copy File	Copy File
<0> Exit To Main Menu	Return to the 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   37691392  Aug/16/2012 07:09:16 N/A    flash:/msr2000.ipe                |
|2   25992     Aug/15/2012 12:18:00 N/A    flash:/startup.mdb              |
|3   1632      Aug/15/2012 12:18:00 M      flash:/startup.cfg              |
|4   84        Aug/15/2012 12:17:59 N/A    flash:/ifindex.dat              |
|5   11029     Aug/15/2012 13:31:16 N/A    flash:/logfile/logfile1.log     |
|6   17        Aug/16/2012 07:47:24 N/A    flash:/.pathfile                |
|7   1006592   Aug/16/2012 07:44:16 M    flash:/msr2000-cmw710-data-a0005.bin|
|8   815       Aug/15/2012 12:03:14 N/A    flash:/license/DeviceID.did     |
|9   1180672   Aug/16/2012 07:44:15 M    flash:/msr2000-cmw710-voice-a0005. bin|
|10  10240     Aug/16/2012 07:44:15 M    flash:/msr2000-cmw710-security-a0005.bin|
|11  24067072  Aug/16/2012 07:44:10 M      flash:/msr2000-cmw710-system-a0005.bin|
|12  11418624  Aug/16/2012 07:44:05 M      flash:/msr2000-cmw710-boot-a0005.bin|
============================================================================
```

Changing the type of a system software image

System software image file attributes include main (M), and backup (B). You can store only one main image, and one backup image on the router. A system software image can have any combination of the M, and B attributes. If the file attribute you are assigning has been assigned to an image, the assignment removes the attribute from that image. The image is marked as N/A if it has only that attribute.

To change the type of a system software image:

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

```
'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                            |
|1   37691392  Aug/16/2012 07:09:16 N/A    flash:/msr2000.ipe                |
|0   Exit                                                                  |
============================================================================
Enter file No:1
```

2. Enter the number of the file you are working with, and press **Enter**.

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

3. Enter a number in the range of 1 to 4 to add or delete a file attribute for the file.

```
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 cfa0:
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
Deleting the file in flash:
 'M' = MAIN      'B' = BACKUP      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                            |
|1   37691392  Aug/16/2012 07:09:16 N/A    flash:/msr2000.ipe                |
|2   25992     Aug/15/2012 12:18:00 N/A    flash:/startup.mdb              |
|3   1632      Aug/15/2012 12:18:00 M      flash:/startup.cfg              |
|4   84        Aug/15/2012 12:17:59 N/A    flash:/ifindex.dat              |
|5   11029     Aug/15/2012 13:31:16 N/A    flash:/logfile/logfile1.log     |
|6   17        Aug/16/2012 07:47:24 N/A    flash:/.pathfile                |
|7   1006592   Aug/16/2012 07:44:16 M      flash:/msr2000-cmw710-data-a0005.bin|
|8   815       Aug/15/2012 12:03:14 N/A    flash:/license/DeviceID.did     |
|9   1180672   Aug/16/2012 07:44:15 M      flash:/msr2000-cmw710-voice-a0005. bin|
|10  10240    Aug/16/2012 07:44:15 M     flash:/msr2000-cmw710-security-a0005.bin|
|11  24067072  Aug/16/2012 07:44:10 M      flash:/msr2000-cmw710-system-a0005.bin|
|12  11418624  Aug/16/2012 07:44:05 M      flash:/msr2000-cmw710-boot-a0005.bin|
0   Exit
Enter file No.:
```

2. Enter the number of the file to delete.

3. When the following prompt appears, enter **Y**.

```
The file you selected is flash:/msr2000-cmw710-security-a0005.bin,Delete it?
[Y/N]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. Check that the storage device has sufficient space for the upgrade file.
6. If the message "Something is wrong with the file" appears, check the file for file corruption.

Appendix C Handling console login password loss

Disabling password recovery capability

Password recovery capability controls console user access to the device configuration and SDRAM from BootWare menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To enhance system security, disable password recovery capability.

Table 14 summarizes options whose availability varies with the password recovery capability setting.

Table 14 BootWare options and password recovery capability compatibility matrix

BootWare menu option	Password recovery enabled	Password recovery disabled	Tasks that can be performed
Download Image Program To SDRAM And Run	Yes	No	Load and run Comware software images in SDRAM.

Skip Authentication for Console Login	Yes	No	Enable console login without authentication.
Skip Current System Configuration	Yes	No	Load the factory-default configuration without deleting the next-startup configuration files.
Restore to Factory Default Configuration	No	Yes	Delete the next-startup configuration files and load the factory-default configuration.

To disable password recovery capability:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Disable password recovery capability.	**undo password-recovery enable**	By default, password recovery capability is enabled.

When password recovery capability is disabled, you cannot downgrade the device software to a version that does not support the capability through the BootWare menus. You can do so at the CLI, but the BootWare menu password configured becomes effective again.

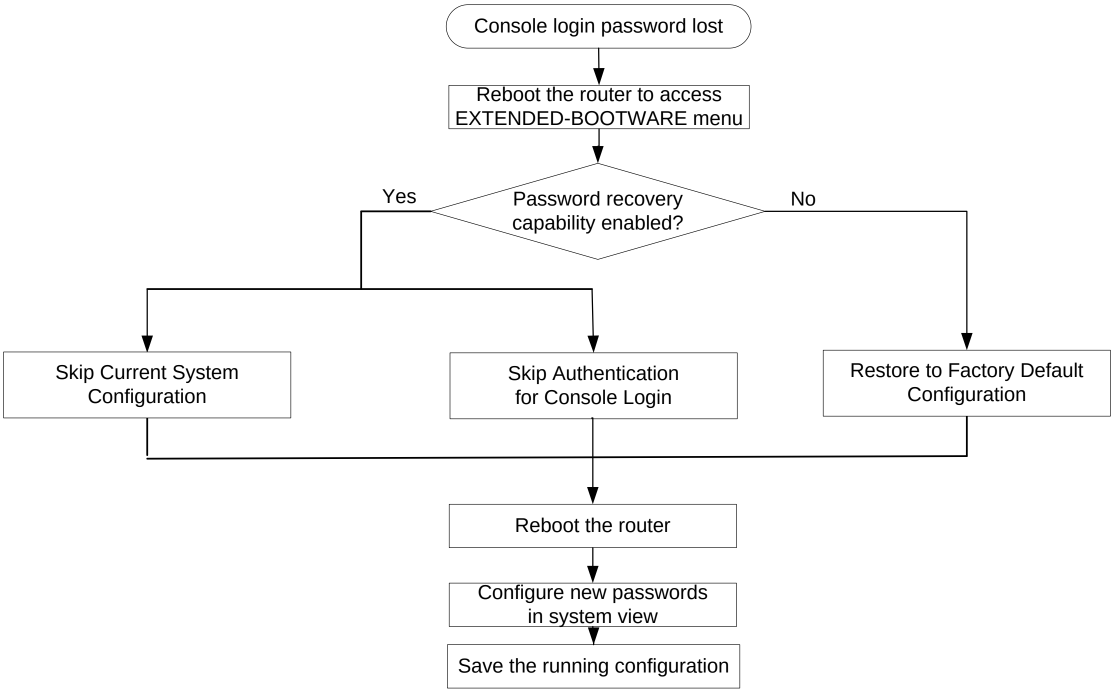
Handling console login password loss

△ **CAUTION:**

Handling console login password loss causes service outage.

The method for handling console login password loss depends on the password recovery capability setting (see Figure 9).

Figure 9 Handling console login password loss


Console login password lost
Reboot the router to access EXTENDED-BOOTWARE menu
Password recovery capability enabled?
Yes
No
Skip Current System Configuration
Skip Authentication for Console Login
Restore to Factory Default Configuration
Reboot the router
Configure new passwords in system view
Save the running configuration

Examining the password recovery capability setting

1. Reboot the router.

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

*****************************************************************************
*                                                                           *
*                   HPE MSR3000 BootWare, Version 1.20                     *
*                                                                           *
*****************************************************************************
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.

Compiled Date       : May 13 2013
CPU ID              : 0x2
Memory Type         : DDR3 SDRAM
Memory Size         : 2048MB
BootWare Size       : 1024KB
Flash Size          : 8MB
cfa0 Size           : 247MB
CPLD Version        : 2.0
PCB Version         : 2.0


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

2. Press **Ctrl + B** within three seconds after the "Press Ctrl+B to access EXTENDED-BOOTWARE MENU..." prompt message appears.
3. Read the password recovery capability setting information displayed before the EXTEND-BOOTWARE menu.

```
Password recovery capability is enabled.
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

===========================<EXTEND-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 EXTEND ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9):
```

Using the Skip Current System Configuration option

1. Reboot the router to access the EXTEND-BOOTWARE menu, and then enter **6**.

```
The current mode is password recovery.
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

===========================<EXTEND-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 EXTEND ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 6
```

   After the configuration skipping flag is set successfully, the following message appears:

```
Flag Set Success.
```

2. When the EXTEND-BOOTWARE menu appears again, enter **1** to reboot the router.

   The router starts up with the factory-default configuration without deleting the next-startup configuration files.

3. To use the configuration in a next-startup configuration file, load the file in system view.

```
<HPE> system-view
[HPE] configuration replace file cfa0:/startup.cfg
Current configuration will be lost, save current configuration? [Y/N]:n
Info: Now replacing the current configuration. Please wait...
Info: Succeeded in replacing current configuration with the file startup.cfg.
```

4. Configure a new console login authentication mode and a new console login password.

   In the following example, the console login authentication mode is password and the authentication password is 123456. For security purposes, the password is always saved in ciphertext, whether you specify the **simple** or **cipher** keyword for the **set authentication password** command.

```
<HPE> system-view
[HPE] line aux 0
[HPE-line-aux0] authentication-mode password
[HPE-line-aux0] set authentication password simple 123456
```

Use the **line aux 0** command on an MSR2000 or MSR 3000 routers. The console port and the AUX port are the same physical port.

Use the **line console 0** command on an MSR4000 routers. An MSR4000 router has a separate console port.

5. To make the settings take effect after a reboot, save the running configuration to the next-startup configuration file.

```
[HPE-line-aux0] save
```

Using the Skip Authentication for Console Login option

1. Reboot the router to access the EXTEND-BOOTWARE menu, and then enter **8**.

```
The current mode is password recovery.
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

===========================<EXTEND-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 EXTEND ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 8
```

The router deletes the console login authentication configuration commands from the main next-startup configuration file. After the operation is completed, the following message appears:

```
Clear Image Password Success!
```

2. When the EXTEND-BOOTWARE menu appears again, enter **1** to reboot the router.

   The router starts up with the main next-startup configuration file.

3. Configure a console login authentication mode and a new console login password. See "Configure a new console login authentication mode and a new console login password.Configure a new console login authentication mode and a new console login password."

4. To make the setting take effect after a reboot, save the running configuration to the next-startup configuration file.

```
[HPE-line-aux0] save
```

Using the Restore to Factory Default Configuration option

△ **CAUTION:**

Using the Restore to Factory Default Configuration option deletes both the main and backup next-configuration files.

1. Reboot the router to access the EXTEND-BOOTWARE menu, and enter **5**.

```
The current mode is no password recovery.
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

===========================<EXTEND-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 EXTEND ASSISTANT MENU
Ctrl+F: Format File System
Enter your choice(0-9): 5
```

2. At the prompt for confirmation, enter **Y**.

   The router deletes its main and backup next-startup configuration files and restores the factory-default configuration.

```
The current mode is no password recovery. The configuration files will be
deleted, and the system will start up with factory defaults, Are you sure to
 continue?[Y/N]Y
Setting...Done.
```

3. When the EXTEND-BOOTWARE menu appears again, enter **1** to reboot the router.

   The router starts up with the factory-default configuration.

4. Configure a new console login authentication mode and a new console login password. See "Configure a new console login authentication mode and a new console login password.Configure a new console login authentication mode and a new console login password.".

5. To make the settings take effect after a reboot, save the running configuration to the next-startup configuration file.

```
[HPE] save
```

HPE MSR954_MSR954P_MSR958-CMW710-R411 Release Notes

Software Feature Changes

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

Contents

Release 0411

None.

Release 0410

This release has the following changes:

New feature: Support of multicast for ADVPN

New feature: Application layer state filtering

New feature: SIP keepalive

New feature: Multicast fast forwarding

New feature: Attack defense policy application to a security zone

New feature: AAA support for IKE extended authentication

New feature: Percentage-based CAR

New feature: Logging OSPF router ID conflict events

New feature: AFT

New feature: Configuring enhanced CC authentication in FIPS mode

New feature: Support of AAA for NETCONF

New feature: Mobile IP tunnel interface settings

New feature: LISP

New feature: LISP tunnel entries and dynamic mobility

New feature: Support of IPv6 multicast routing for VPN instances

New feature: LISP virtual machine multi-hop mobility and DDT

New feature: LISP NSR

New feature: PPPoE client support for IPv6

New feature: DPI engine and content filtering

New feature: IPS

New feature: NBAR

New feature: URL filtering

New feature: Local portal Web server

New feature: Support of portal for NETCONF

New feature: Newly-added MIB objects

New feature: IPS, ACG, and SSL VPN licenses

New feature: Support of NQA for NETCONF

New feature: Configuring CWMP to support VPN

New feature: Transceiver module source alarm

New feature: VLAN interface performance optimization

New feature: NAT support for multicast source address in PIM join/prune packets

New feature: GDOI GM group anti-replay window

New feature: SIP compatibility

New feature: Voice VLAN

New feature: L2TP-based EAD

New feature: BFD for an aggregation group

New feature: 4G modem IMSI/SN binding authentication

New feature: Media Stream Control (MSC) logging

New feature: IMSI/SN binding authentication

New feature: Specifying a band for a 4G modem

New feature: Using tunnel interfaces as OpenFlow ports

New feature: NETCONF support for ACL filtering

New feature: WAAS

New feature: Support for the MKI field in SRTP or SRTCP packets

New feature: SIP domain name

New feature: Setting the maximum size of advertisement files

New feature: Support of VCF for NETCONF

New feature: Support of SNMP for NETCONF

New feature: Support of file system for NETCONF

New feature: Support of PoE for NETCONF

New feature: Support of RMON for NETCONF

New feature: Support of policy-based routing for NETCONF

New feature: Support of BGP for NETCONF

New feature: Support of OSPF for NETCONF

New feature: Support of ping for NETCONF

New feature: Support of tracert for NETCONF

New feature: Support of L2VPN for NETCONF

New feature: SIP support for VRF

New feature: IKEv2

New feature: Specifying an IKEv2 profile for an IPsec policy

New feature: Bidirectional BFD control detection for RIP

New feature: OSPF router ID autoconfiguration

New feature: Associating a static route with a track entry

New feature: VLAN tag processing rule for incoming traffic

New feature: IP-based portal-free rule

New feature: Portal redirect packet statistics

New feature: GDVPN

New feature: OpenFlow instance

New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set

New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy

New feature: SIP session refresh

Modified feature: User profile

Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes

Modified feature: PKI certificate auto-renewal

Modified feature: Configuring the PKI entity DN

Modified feature: ADVPN

Modified feature: Telnet redirect

Modified feature: DHCP snooping performance optimization

Modified feature: OSPF performance optimization

Modified feature: IP performance optimization

Modified feature: AAA

Modified feature: Configuring a cellular interface for a 3G/4G modem

Modified feature: QoS on VXLAN tunnel interfaces

Modified feature: Option 60 encapsulation in DHCP replies

Modified feature: MPLS QoS support for matching the EXP field

Modified feature: MPLS QoS support for marking the EXP field

Modified feature: Automatic configuration

Modified feature: User profile

Modified feature: Default size of the TCP receive and send buffer

Modified feature: Support for per-packet load sharing

Modified feature: Default user role

Modified feature: Debugging

Modified feature: SSH username

Modified feature: IS-IS hello packet sending interval

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Modified feature: Saving, rolling back, and loading the configuration

Modified feature: Displaying information about SSH users

Modified feature: SIP trusted nodes

Modified feature: IPsec ESP encryption algorithms

Modified feature: IPsec ESP authentication algorithms

Modified feature: IPsec AH authentication algorithms

Modified feature: Specifying an encryption algorithm for an IKE proposal

Modified feature: Specifying an authentication algorithm for an IKE proposal

Modified feature: Generating asymmetric key pairs

Modified feature: Specifying an ECDSA key pair for certificate request

Modified feature: QoS MIB

Modified feature: Enabling PFS for an IPsec transform set

Modified feature: Displaying track entry infomration

Removed feature: Tiny proxy

Removed feature: Displaying switching fabric channel usage

New feature: Support of multicast for ADVPN

Configuring support of multicast for ADVPN

For information about this feature, see IPv4/IPv6 PIM and IPv4/IPv6 multicast routing and forwarding in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide.*

Command reference

The following commands were added:

- **display ipv6 pim nbma-link**.
- **display pim nbma-link**.
- **ipv6 pim nbma-mode**.
- **pim nbma-mode**.

ADVPN multicast parameters were added to the following commands:

- **display ipv6 multicast forwarding df-info**.
- **display ipv6 multicast forwarding-table**.
- **display ipv6 multicast routing-table**.
- **display ipv6 pim df-info**.
- **display ipv6 pim routing-table**.
- **display multicast forwarding df-info**.
- **display multicast forwarding-table**.
- **display multicast routing-table**.
- **display pim df-info**.
- **display pim routing-table**.

For information about the commands, see IPv4/IPv6 PIM and IPv4/IPv6 multicast routing and forwarding commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference.*

New feature: Application layer state filtering

Configuring application layer state filtering

For information about this feature, see ASPF in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following keywords were added to the **detect** command:

- **dns**.
- **http**.
- **smtp**.
- **action**.
- **drop**.

The fields that indicate application layer status were added to the output from the **display aspf policy** command.

For information about the commands, see ASPF in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: SIP keepalive

Configuring SIP keepalive

You can configure in-dialog keepalive and out-of-dialog keepalive.

Command reference

New command: options-ping

Use **options-ping** to globally enable in-dialog keepalive.

Use **undo options-ping** to globally disable in-dialog keepalive.

Syntax

options-ping *seconds*

undo options-ping

Default

In-dialog keepalive is disabled globally.

View

SIP view

Predefined use roles

network-admin

Parameters

seconds: Specifies the global interval for sending OPTIONS messages during a session, in the range of 60 to 1200 seconds.

Usage guidelines

This command enables the device to periodically send OPTIONS messages at the specified interval to monitor the status of the remote SIP UA during a session. It does not take effect when the session refresh negotiation succeeds before a call is established.

If you disable this feature, the device does not send OPTIONS messages after a call is established.

Example

# Globally enable in-dialog keepalive and set the interval to 60 seconds for sending OPTIONS messages during a session.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] options-ping 60
```

New command: voice-class sip options-ping

Use **voice-class sip options-ping** to enable in-dialog keepalive for a VoIP entity.

Use **voice-class sip options-ping** to disable in-dialog keepalive for a VoIP entity.

Syntax

voice-class sip options-ping { **global** | *seconds* }

undo voice-class sip options-ping

Default

A VoIP entity uses the global configuration for in-dialog keepalive.

Views

VoIP entity view

Predefined user roles

network-admin

Parameters

global: Applies the global configuration for in-dialog keepalive to the VoIP entity.

seconds: Specifies the interval for sending OPTIONS messages during a session, in the range of 60 to 1200 seconds.

Usage guidelines

For a VoIP entity, the entity-specific in-dialog keepalive interval takes priority over the global in-dialog keepalive interval set in SIP view.

Examples

# Enable in-dialog keepalive for VoIP entity 1 and set the interval to 60 seconds for sending OPTIONS messages during a session.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip options-ping 60
```

# Apply the global configuration for in-dialog keepalive to VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip options-ping global
```

New feature: Multicast fast forwarding

Configuring multicast fast forwarding

In this release, the router supports multicast fast forwarding.

Command reference

New command: display multicast fast-forwarding cache

Use **display multicast fast-forwarding cache** to display information about multicast fast forwarding entries.

Syntax

Centralized devices:

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* **|** *group-address*] *

Distributed devices in standalone mode:Centralized IRF devices:

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* **|** *group-address*] * [**slot** *slot-number*]

Distributed devices in IRF mode:

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* **|** *group-address*] * [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command displays multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Display multicast fast forwarding entries on the public network.

```
<Sysname> display multicast fast-forwarding cache
Total 1 entries, 1 matched
(60.1.1.200, 225.0.0.2)
Status : Enabled
Source port: 2001 Destination port: 2002
Protocol : 2 Flag : 0x2
Incoming interface: GigabitEthernet1/0/3
List of 1 outgoing interfaces:
GigabitEthernet1/0/2
Status: Enabled Flag: 0x14
```

Table 1 **Command output**

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the multicast fast forwarding table, and the total number of matching (S, G) entries.
(60.1.1.200, 225.0.0.2)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The interface is added to the entry because of packets passed through between cards. • **0x2**—The interface is added to an existing entry. • **0x4**—The MAC address of the interface is needed for fast forwarding. • **0x8**—The interface is an outgoing interface associated with the incoming VLAN or super VLAN interface. • **0x10**—The interface is associated with the entry. • **0x20**—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • **Enabled**—Available. • **Disabled**—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

New command: reset multicast fast-forwarding cache

Use **reset multicast fast-forwarding cache** to clear multicast fast forwarding entries.

Syntax

Centralized devices:

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** }

Distributed devices in standalone mode:Centralized IRF devices:

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** } [**slot** *slot-number*]

Distributed devices in IRF mode:

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** } [**chassis** *chassis-number* **slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command clears multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Clear all multicast fast forwarding entries on the public network.

```
<Sysname> reset multicast fast-forwarding cache all
```

# Clear the multicast fast forwarding entry for multicast source and group (20.0.0.2, 225.0.0.2) on the public network.

```
<Sysname> reset multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

New command: display ipv6 multicast fast-forwarding cache

Use **display ipv6 multicast fast-forwarding cache** to display information about IPv6 multicast fast forwarding entries.

Syntax

Centralized devices:

display ipv6 multicast [vpn-instance *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* | *ipv6-group-address*] *

Distributed devices in standalone mode:Centralized IRF devices:

display ipv6 multicast [vpn-instance *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* | *ipv6-group-address*] * [**slot** *slot-number*]

Distributed devices in IRF mode:

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* | *ipv6-group-address*] * [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers from 0 to F.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays IPv6 multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command displays IPv6 multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Display IPv6 multicast fast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast fast-forwarding cache
Total 1 entries, 1 matched

(FE1F:60::200, FF0E::1)
Status      : Enabled
Source port: 2001                    Destination port: 2002
Protocol    : 2                      Flag             : 0x2
Incoming Interfacfe: GigabitEthernet1/0/3
List of 1 outgoing interfaces:
GigabitEthernet1/0/2
Status: Enabled                Flag: 0x14
```

Table 2 **Command output**

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the IPv6 multicast fast forwarding table, and the total number of matching (S, G) entries.
(FE1F:60::200, FF0E::1)	(S, G) entry.
Protocol	Protocol number.

Field	Description
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by IPv6 multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The interface is added to the entry because of packets passed through between cards. • **0x2**—The interface is added to an existing entry. • **0x4**—The MAC address of the interface is needed for fast forwarding. • **0x8**—The interface is an outgoing interface associated with the incoming VLAN or super VLAN interface. • **0x10**—The interface is associated with the entry. • **0x20**—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • **Enabled**—Available. • **Disabled**—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

New command: reset ipv6 multicast fast-forwarding cache

Use **reset ipv6 multicast fast-forwarding cache** to clear IPv6 multicast fast forwarding entries.

Syntax

Centralized devices:

reset ipv6 multicast [vpn-instance *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** }

Distributed devices in standalone mode:Centralized IRF devices:

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**slot** *slot-number*]

Distributed devices in IRF mode:

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers from 0 to F.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears IPv6 multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command clears IPv6 multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Clear all IPv6 multicast fast forwarding entries on the public network

```
<Sysname> reset ipv6 multicast fast-forwarding cache all
```

# Clear the IPv6 multicast fast forwarding entry for IPv6 multicast source and group (FE1F:20::2, FF0E::1) on the public network.

```
<Sysname> reset ipv6 multicast fast-forwarding cache fe1f:20::2 ff0e::1
```

New feature: Attack defense policy application to a security zone

Applying an attack defense policy to a security zone

To apply an attack defense policy to a security zone:

Step	Command	Remarks
3. Enter system view.	**system-view**	N/A
4. Enter security zone view.	**security-zone name** *Trust*	N/A
5. Apply an attack defense policy to the security zone.	**attack-defense apply policy** *policy-number*	By default, a security zone has no attack defense policy applied.

Command reference

The following commands were newly added:

- **attack-defense apply policy**
- **blacklist enable**
- **client-verify dns enable**
- **client-verify http enable**
- **client-verify tcp enable**

- **display attack-defense flood statistics ip**
- **display attack-defense flood statistics ipv6**
- **display attack-defense scan attacker ip**
- **display attack-defense scan attacker ipv6**
- **display attack-defense scan attacker ipv6**
- **display attack-defense scan victim ipv6**
- **display attack-defense statistics security-zone**
- **reset attack-defense statistics security-zone**

For information about the commands, see attack defense commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: AAA support for IKE extended authentication

Configuring IKE extended authentication

For information about this feature, see AAA configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **authentication ike** command was newly added.

The **ike** keyword was added to the **display local-user**, **undo local-user**, **service-type**, and **undo service-type** commands.

For information about the commands, see AAA commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Percentage-based CAR

Configuring percentage-based CAR

For information about this feature, see QoS in *H3C MSR Router Series Comware 7 ACL and QoS Configuration Guide*.

Command reference

The **percent car** command was added.

For information about the command, see traffic behavior commands in *H3C MSR Router Series Comware 7 ACL and QoS Command Reference*.

New feature: Logging OSPF router ID conflict events

Logging OSPF router ID conflict events

For information about this feature, see OSPF configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide*.

Command reference

The following commands were newly added:

- **database-filter peer** (OSPF view)
- **ospf database-filter**
- **ospf ttl-security**
- **ttl-security**

For information about the commands, see OSPF commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: AFT

Configuring AFT

For information about this feature, see AFT in *H3C MSR Router Series Comware 7 Layer 3—IP Services Configuration Guide*.

Command reference

For information about the commands, see AFT commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Configuring enhanced CC authentication in FIPS mode

Configuring enhanced CC authentication in FIPS mode

For information about this feature, see IPsec, SSH, SSL, and public key management in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **ecdsa** keyword was added to the following commands:

- **scp**.
- **scp ipv6**.
- **sftp**.
- **sftp ipv6**.
- **ssh2**.
- **ssh2 ipv6**.

The **dhe_rsa_aes_128_cbc_sha** and **dhe_rsa_aes_256_cbc_sha** keywords were removed from the **ciphersuite** command in FIPS mode.

The **secp192r1** and **secp256r1** keywords were added to the **public-key local create** command.

The **public-key local export ecdsa** command was added.

For more information about these commands, see IPsec, SSH, SSL, and public key management commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Support of AAA for NETCONF

Configuring support of AAA for NETCONF

For information about this feature, see AAA in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **radius session-control client** command was newly added. The **security-policy-server** command was deleted.

For information about the command, see AAA commands in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

New feature: Mobile IP tunnel interface settings

Configuring the mobile IP tunnel interface settings

Step	Command	Remarks
6. Enter system view.	**system-view**	N/A
7. Enable the mobile router feature and enter mobile router view.	**ip mobile router**	By default, the mobile router feature is disabled.
8. Assign a home address to the mobile router.	**address** *ip-address*	By default, the mobile router does not have any home addresses.
9. Specify the IP address of the home agent for the mobile router.	**home-agent** *ip-address*	By default, no home agent is specified for the mobile router.
10. (Optional.) Set the MTU for the mobile IP tunnel interface.	**tunnel mtu** *value*	By default, the MTU for the tunnel interface is 64000 bytes.
11. (Optional.) Set the DF bit to 0 for outgoing tunneled packets.	**ip df-bit zero**	By default, the DF bit of outgoing tunneled packets is not set.
12. (Optional.) Apply an IPsec policy to the mobile IP tunnel interface.	**ipsec policy** *policy-name*	By default, no IPsec policy is applied to the mobile IP tunnel interface.
13. (Optional.) Set the TCP MSS for the mobile IP tunnel interface.	**tcp mss** *value*	By default, no TCP MSS is set.

Command reference

The following commands were added:

- **ip df-bit zero**
- **ipsec policy**
- **tcp mss**

For information about the commands, see NEMO commands in *H3C MSR Router Series Comware 7 NEMO Command Reference*.

New feature: LISP

Configuring LISP

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

For information about the commands, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: LISP tunnel entries and dynamic mobility

Configuring LISP tunnel entries and dynamic mobility

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

For information about the commands, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: Support of IPv6 multicast routing for VPN instances

Enabling support of IP multicast routing for VPN instances

For information about this feature, see IPv6 multicast routing and forwarding in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide.*

Command reference

The **ipv6 multicast routing vpn-instance** command was added.

For information about the command, see IPv6 multicast routing and forwarding commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference.*

New feature: LISP virtual machine multi-hop mobility and DDT

Configuring LISP virtual machine multi-hop mobility and DDT

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

The **eid-notify** command was newly added.

For information about the command, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: LISP NSR

Configuring LISP NSR

The **display system internal lisp forwarding statistics** command was added. You can use the command to display the LISP thread statistics.

The **display system internal lisp nsr no-cache** command was added. You can use the command to display the tentative entries created during the NSR active/standby switchover.

The **display system internal lisp nsr status** command was added. You can use the command to display the LISP NSR status.

Command reference

The following commands were newly added:

- **display system internal lisp forwarding statistics**
- **display system internal lisp nsr no-cache**
- **display system internal lisp nsr status**

For information about the commands, see LISP probe commands in *H3C MSR Router Series Comware 7 Probe Command Reference*.

New feature: PPPoE client support for IPv6

Associating a dial rule with a dialup interface

For information about this feature, see DDR in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Configuration Guide*.

Command reference

The **ipv6** keyword is added to the **dialer-group rule** command. For information about this command, see DDR commands in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Command Reference*.

Specifying an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address

For information about this feature, see IPv6 basics in *H3C MSR Router Series Comware 7 Layer 3—IP Services Configuration Guide*.

Command reference

The **ipv6 address** command is added. For information about the command, see IPv6 basics commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: DPI engine and content filtering

Configuring the DPI engine and content filtering

For information about this feature, see DPI overview and DPI engine in *H3C MSR Router Series Comware 7 DPI Configuration Guide.*

Command reference

For information about the commands, see DPI overview and DPI engine commands in *H3C MSR Router Series Comware 7 DPI Command Reference.*

New feature: IPS

Configuring IPS

For information about this feature, see IPS configuration in *H3C MSR Router Series Comware 7 DPI Configuration Guide.*

Command reference

For information about the commands, see IPS commands in *H3C MSR Router Series Comware 7 DPI Command Reference.*

New feature: NBAR

Configuring NBAR

For information about this feature, see APR in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following new commands were added:

- **apr signature update**.
- **Description**.
- **Destination**.
- **Direction**.
- **Disable**.
- **display app-group**.
- **display application**.
- **display apr signature information**.
- **include app-group**.
- **nbar application**.
- **nbar protocol-discovery**.
- **service-port**.
- **signature**.
- **source**.

For information about the commands, see APR in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: URL filtering

Configuring URL filtering

For information about this feature, see URL filtering configuration in *H3C MSR Router Series Comware 7 DPI Configuration Guide.*

Command reference

For information about the commands, see URL filtering commands in *H3C MSR Router Series Comware 7 DPI Command Reference.*

New feature: Local portal Web server

Configuring a local portal Web server

For information about this feature, see portal in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The following commands were added:

- **portal local-web-server**
- **default-logon-page**
- **logon-page**
- **tcp-port**

The **ssid** keyword was added to the **url-parameter** *param-name* { **apmac** | **original-url** | **source-address** | **source-mac** | **ssid** | **value** *expression* } command.

For information about the commands, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Support of portal for NETCONF

Support for NETCONF was added to portal.

New feature: Newly-added MIB objects

Event MIB added support for the hh3cWirelessCardModemMode and hh3cWirelessCardCurNetConn MIB objects.

New feature: IPS, ACG, and SSL VPN licenses

This release added support for IPS, ACG and SSL VPN licenses.

New feature: Support of NQA for NETCONF

Support for NETCONF was added to NQA.

New feature: Configuring CWMP to support VPN

Configuring CWMP to support VPN

For information about this feature, see CWMP configuration in *H3C MSR Router Series Comware 7 Network Management and Monitoring Configuration Guide*.

Command reference

For information about the commands, see CWMP commands in *H3C MSR Router Series Comware 7 Network Management and Monitoring Command Reference*.

New feature: Transceiver module source alarm

Disabling transceiver module source alarm

For information about this feature, see device management in *H3C MSR Router Series Comware 7 Fundamentals Configuration Guide*.

Command reference

transceiver phony-alarm-disable

For information about this command, see device management commands in *H3C MSR Router Series Comware 7 Fundamentals Command Reference*.

New feature: VLAN interface performance optimization

This software version optimized the following items:

- VLAN functions used for sending data in the adaption layer.
- Processing flow of the RAW functions for sending and receiving data for chips mv88ex, mvcpss, and bcm5614x.

New feature: NAT support for multicast source address in PIM join/prune packets

This feature enables the device to act as a NAT gateway and perform NAT on the multicast source address in PIM join or prune packets based on NAT mappings. Use this feature in a multicast scenario where the multicast source resides on a private network, multicast receivers reside on private networks, and PIM-SSM mode is used.

New feature: GDOI GM group anti-replay window

Configuring the anti-replay window for a GDOI GM group

Step	Command	Remarks
14. Enter system view.	**system-view**	N/A
15. Create a GDOI GM group and enter GDOI GM group view.	**gdoi gm group** [**ipv6**] *group-name*	By default, no GDOI GM groups exist.

Step	Command	Remarks
16. (Optional.) Set the anti-replay window size for the GDOI GM group.	**client anti-replay window** { **sec** *seconds* | **msec** *milliseconds* }	By default, the anti-replay window size is not set for a GDOI GM group.

Command reference

client anti-replay window

Use **client anti-replay window** to set the anti-replay window size for a GDOI GM group.

Use **undo client anti-replay window** to restore the default.

Syntax

client anti-replay window { **sec** *seconds* | **msec** *milliseconds* }

undo client anti-replay window

Default

The anti-replay window size is not set for a GDOI GM group.

Views

GDOI GM group view

Predefined user roles

network-admin

Parameters

sec *seconds*: Specifies the anti-replay window size in seconds in the range of 1 to 100.

msec *milliseconds*: Specifies the anti-replay window size in milliseconds in the range of 100 to 10000.

Usage guidelines

The anti-replay window size set in this command takes priority over the anti-replay window size obtained from the KS. If you do not configure this command, the anti-replay window size obtained from the KS is used.

This command must be used together with the Cisco IP-D3P feature.

Examples

# Set the anti-replay window size to 50 seconds for GDOI GM group **group1**.

```
<Sysname> system-view
[Sysname] gdoi gm group group1
[Sysname-gdoi-gm-group-group1] client anti-replay window sec 50
```

New feature: SIP compatibility

Configuring SIP compatibility

If a third-party device does not implement SIP in strict accordance with the RFC standard, you can configure SIP compatibility for the router to interoperate with the third-party device.

With the **sip-compatible t38** command configured, the router excludes **:0** from the following SDP parameters in the originated re-INVITE messages:

- T38FaxTranscodingJBIG.
- T38FaxTranscodingMMR.
- T38FaxFillBitRemoval.

With the **sip-compatible x-param** command configured, the router adds SDP description information (a=X-fax and a=X-modem) for fax pass-through and modem pass-through in the originated re-INVITE messages.

To configure SIP compatibility:

Step	Command	Remarks
17. Enter system view.	**system-view**	N/A
18. Enter voice view.	**voice-setup**	N/A
19. Enter SIP view.	**sip**	N/A
20. Configure SIP compatibility.	**sip-compatible** { **t38** | **x-param** }	By default, SIP compatibility is not configured.

Command reference

New command:sip-compatible

Use **sip-compatible** to configure SIP compatibility with a third-party device.

Use **undo sip-compatible** to restore the default.

Syntax

sip-compatible { **t38** | **x-param** }

undo sip-compatible { **t38** | **x-param** }

Default

SIP compatibility is not configured.

Views

SIP view

Predefined user roles

network-admin

Parameters

t38: Configures SIP compatibility for standard T.38 fax. With this keyword specified, the router excludes **:0** from the following SDP parameters in the originated re-INVITE messages:

- T38FaxTranscodingJBIG.
- T38FaxTranscodingMMR.
- T38FaxFillBitRemoval.

This keyword is required when the router interoperates with a third-party softswitch device to exchange T.38 fax messages.

x-param: Configures SIP compatibility for fax pass-through and modem pass-through. With this keyword specified, the router adds SDP description information for fax pass-through and modem pass-through to outgoing re-INVITE messages. This keyword is required when the router interoperates with a third-party softswitch device to perform fax pass-through and modem pass-through.

Usage guidelines

The **t38** and **x-param** keywords can be both configured to interoperate with a third-party softswitch device.

Examples

# Configure SIP compatibility for standard T.38 fax.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-compatible t38
```

New feature: Voice VLAN

Configuring a voice VLAN

Configuring a port to operate in automatic voice VLAN assignment mode

Step	Command	Remarks
21. Enter system view.	**system-view**	N/A
22. (Optional.) Set the voice VLAN aging timer.	**voice-vlan aging** *minutes*	By default, the aging timer of a voice VLAN is 1440 minutes.
23. (Optional.) Enable the voice VLAN security mode.	**voice-vlan security enable**	By default, the voice VLAN security mode is enabled.

Step	Command	Remarks
24. (Optional.) Add an OUI address for voice packet identification.	**voice-vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	By default, system default OUI addresses exist.
25. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter S-channel interface view: **interface s-channel** *interface-number.channel-id* • Enter S-channel aggregate interface view: **interface schannel-aggregation** *interface-number*:*channel-id* • Enter Layer 2 RPR logical interface view: **interface rpr-bridge** *interface-number*	N/A
26. Set the link type of the port.	• Set the port link type to trunk: **port link-type trunk** • Set the port link type to hybrid: **port link-type hybrid**	N/A
27. Configure the port to operate in automatic voice VLAN assignment mode.	**voice-vlan mode auto**	By default, the automatic voice VLAN assignment mode is enabled.
28. Enable the voice VLAN feature on the port.	**voice-vlan** *vlan-id* **enable**	By default, the voice VLAN feature is disabled on a port. Before you execute this command, make sure the specified VLAN already exists.

Configuring a port to operate in manual voice VLAN assignment mode

Step	Command	Remarks
29. Enter system view.	**system-view**	N/A
30. (Optional.) Enable the voice VLAN security mode.	**voice-vlan security enable**	By default, the voice VLAN security mode is enabled.
31. (Optional.) Add an OUI address for voice packet identification.	**voice-vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	By default, system default OUI addresses exist.

Step	Command	Remarks
32. Enter interface view.	• Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* • Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* • Enter S-channel interface view: **interface s-channel** *interface-number.channel-id* • Enter S-channel aggregate interface view: **interface schannel-aggregation** *interface-number*:*channel-id* • Enter Layer 2 RPR logical interface view: **interface rpr-bridge** *interface-number*	N/A
33. Configure the port to operate in manual voice VLAN assignment mode.	**undo voice-vlan mode auto**	By default, a port operates in automatic voice VLAN assignment mode.
34. Set the link type of the port.	• Set the port link type to access: **port link-type access** • Set the port link type to trunk: **port link-type trunk** • Set the port link type to hybrid: **port link-type hybrid**	By default, each port is an access port.
35. Assign the access, trunk, or hybrid port to the voice VLAN.	• For the access port: **port access vlan** *vlan-id* • For the trunk port: **port trunk permit vlan** { *vlan-id-list* | **all** } • For the hybrid port: **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	After you assign an access port to the voice VLAN, the voice VLAN becomes the PVID of the port.
36. (Optional.) Configure the voice VLAN as the PVID of the trunk or hybrid port.	• For the trunk port: **port trunk pvid vlan** *vlan-id* • For the hybrid port: **port hybrid pvid vlan** *vlan-id*	This step is required for untagged incoming voice traffic and prohibited for tagged incoming voice traffic.
37. Enable the voice VLAN feature on the port.	**voice-vlan** *vlan-id* **enable**	By default, the voice VLAN feature is disabled on a port. Before you execute this command, make sure the specified VLAN already exists.

Enabling LLDP for automatic IP phone discovery

Step	Command	Remarks
38. Enter system view.	**system-view**	N/A
39. Enable LLDP for automatic IP phone discovery.	**voice-vlan track lldp**	By default, LLDP for automatic IP phone discovery is disabled.

Configuring LLDP to advertise a voice VLAN

For IP phones that support LLDP, the device advertises the voice VLAN information to the IP phones through LLDP-MED TLVs.

To configure LLDP to advertise a voice VLAN:

Step	Command	Remarks
40. Enter system view.	**system-view**	N/A
41. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
42. Configure an advertised voice VLAN ID.	**lldp tlv-enable med-tlv network-policy** *vlan-id*	By default, no advertised voice VLAN ID is configured.

Configuring CDP to advertise a voice VLAN

If an IP phone supports CDP but does not support LLDP, it sends CDP packets to the device to request the voice VLAN ID. If the IP phone does not receive the voice VLAN ID within a time period, it sends out untagged voice packets. These untagged voice packets cannot be differentiated from other types of packets.

You can configure CDP compatibility on the device to enable it to perform the following operations:

- Receive and identify CDP packets from the IP phone.
- Send CDP packets to the IP phone. The voice VLAN information is carried in the CDP packets.

After receiving the advertised VLAN information, the IP phone starts automatic voice VLAN configuration. Packets from the IP phone will be transmitted in the dedicated voice VLAN.

To configure CDP to advertise a voice VLAN:

Step	Command	Remarks
43. Enter system view.	**system-view**	N/A
44. Enable CDP compatibility.	**lldp compliance cdp**	By default, CDP compatibility is disabled.
45. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
46. Configure CDP-compatible LLDP to operate in TxRx mode.	**lldp compliance admin-status cdp txrx**	By default, CDP-compatible LLDP operates in **disable** mode.
47. Configure an advertised voice VLAN ID.	**cdp voice-vlan** *vlan-id*	By default, no advertised voice VLAN ID is configured.

Displaying and maintaining voice VLANs

Execute **display** commands in any view.

Task	Command
Display the voice VLAN state.	**display voice-vlan state**
Display OUI addresses on a device.	**display voice-vlan mac-address**

Command reference

The following commands were added:

- **display voice-vlan mac-address**.
- **display voice-vlan state**.
- **voice-vlan aging**.
- **voice-vlan enable**.
- **voice-vlan mac-address**.
- **voice-vlan mode auto**.
- **voice-vlan security enable**.
- **voice-vlan track lldp**.

For more information about these commands, see *H3C MSR Series Routers Layer 2—LAN Switching Command Reference(V7)*.

New feature: L2TP-based EAD

Enabling L2TP-based EAD

EAD authenticates PPP users that pass the access authentication. PPP users that pass EAD authentication can access network resources. PPP users that fail EAD authentication can only access the resources in the quarantine areas.

EAD uses the following procedure:

1. The iNode client uses L2TP to access the LNS. After the client passes the PPP authentication, the CAMS/IMC server assigns isolation ACLs to the LNS. The LNS uses the isolation ACLs to filter incoming packets.
2. After the IPCP negotiation, the LNS sends the IP address of the CAMS/IMC server to the iNode client. The server IP address is permitted by the isolation ACLs.
3. The CAMS/IMC sever authenticates the iNode client and performs security check for the iNode client. If the iNode client passes security check, the CAMS/IMC server assigns security ACLs for the iNode client to the LNS. The iNode client can access network resources.

To enable L2TP-based EAD:

Step	Command	Remarks
48. Enter system view.	**system-view**	N/A
49. Create a VT interface and enter its view	**interface virtual-template** *virtual-template-number*	N/A
50. Enable L2TP-based EAD.	**ppp access-control enable**	By default, L2TP-based EAD is disabled.

Command reference

ppp access-control enable

Use **ppp access-control enable** to enable L2TP-based EAD.

Use **undo ppp access-control enable** to disable L2TP-based EAD.

Syntax

ppp access-control enable

undo ppp access-control enable

Default

L2TP-based EAD is disabled.

Views

VT interface view

Predefined user roles

network-admin

Usage guidelines

This command does not apply to VA interfaces that already exist in the VT interface. It only applies to newly created VA interfaces.

Different ACLs are required for different users if the VT interface is used as the access interface for the LNS.

After L2TP-based EAD is enabled, the LNS transparently passes CAMS/IMC packets to the iNode client to inform the client of EAD server information, such as the IP address.

Examples

# Enable L2TP-based EAD.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] ppp access-control enable
```

display ppp access-control interface

Use **display ppp access-control interface** to display access control information for VA interfaces on a VT interface.

Syntax

display ppp access-control interface { *interface-type interface-number* **|** *interface-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

interface-name: Specifies an interface by its name.

Examples

# Display access control information for VA interfaces on VT interface 2.

```
<Sysname> display ppp access-control interface virtual-template 2
Interface: Virtual-Template2:0
  User Name: mike
  In-bound Policy: acl 3000
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.

  Interface: Virtual-Template2:1
  User Name: tim
  In-bound Policy: acl 3001
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

Table 3 **Command output**

Field	Description
Interface	VA interface that the PPP user accesses.
User Name	Username of the PPP user.
In-bound Policy	Security ACLs for the PPP user.
Totally x packets, x bytes, x% permitted	Total number, data rate, and pass percentage of permitted packets.
Totally x packets, x bytes, x% denied	Total number, data rate, and reject percentage of denied packets.

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 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 *H3C MSR Router Series Comware 7 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 source and destination IP addresses cannot be the same.
- The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode.
- As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.

- Make sure the number of member ports in a BFD-enabled aggregation group is not larger than the number of BFD sessions supported by the device. Otherwise, this command might cause some Selected ports in the aggregation group to change to the Unselected state.

Configuration procedure

To enable BFD for an aggregation group:

Step	Command	Remarks
51. Enter system view.	**system-view**	N/A
52. Enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	N/A
53. 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 unicast source IP address of BFD sessions. The source IP address cannot be 0.0.0.0.

destination *ip-address*: Specifies the unicast destination IP address of BFD sessions. The destination IP address cannot be 0.0.0.0.

Usage 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 source and destination IP addresses cannot be the same.

The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode. For more information about BFD, see *H3C MSR Router Series Comware 7 High Availability Configuration Guide*.

As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.

Make sure the number of member ports in a BFD-enabled aggregation group is not larger than the number of BFD sessions supported by the device. Otherwise, this command might cause some Selected ports in the aggregation group to change to the Unselected state.

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: 4G modem IMSI/SN binding authentication

This feature includes the IMSI/SN information in the 4G dial-up authentication information.

Command reference

apn

Use **apn** to create an access point name (APN).

Use **undo apn** to remove an APN.

Syntax

apn { **dynamic** | **static** *apn* }

undo apn

Default

No APN is configured.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

dynamic: Uses an APN automatically assigned by the service provider.

static *apn*: Specifies the APN provided by the service provider. It is a string of 1 to 100 characters. Whether the string is case-sensitive varies by service providers.

Usage guidelines

You must specify an APN for a 4G dial-up profile.

Examples

# Specify the APN **apn1** for the 4G dial-up profile **test**.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] apn static apn1
```

apn-profile

Use **apn-profile** to create a 4G dial-up profile.

Use **undo apn-profile** to remove a 4G dial-up profile.

Syntax

apn-profile *profile-name*

undo apn-profile *profile-name*

Default

No 4G dial-up profiles are configured.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a 4G dial-up profile name.

Usage guidelines

A 4G dial-up profile takes effect only after you associate the profile with a 4G interface. To remove a 4G dial-up profile, you must first remove the association between the profile and the 4G interface.

Examples

# Create the 4G dial-up profile **test**.

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

```
[Sysname] apn-profile test
```

apn-profile apply

Use **apn-profile apply** to specify a 4G dial-up profile.

Use **undo apn-profile apply** to restore the default.

Syntax

apn-profile apply *profile-name* [**backup** *profile-name*]

undo apn-profile apply

Default

No 4G dial-up profiles are specified.

Views

Eth-channel interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a primary 4G dial-up profile name.

backup *profile-name*: Specifies a backup 4G dial-up profile name.

Usage guidelines

After you specify a 4G dial-up profile for a 4G modem, the 4G modem uses the settings in the profile to negotiate with the service provider's device.

The primary profile always has priority over the backup profile. For each dialup connection establishment, the 4G modem uses the backup profile only when it has failed to dial up using the primary profile.

This command takes effect only on dialup connections initiated after the command is configured. It does not take effect on a dialup connection that has been established.

Examples

# Specify the primary 4G dial-up profile **test** and the backup 4G dial-up profile **bktest** for Eth-channel interface 2/4/0:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 2/4/0:0
[Sysname-Eth-channel2/4/0:0] apn-profile apply test backup bktest
```

attach-format

Use **attach-format** to set a separator for the authentication information to be sent.

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

Syntax

attach-format imsi-sn split *splitchart*

undo attach-format imsi-sn split

Default

No separator is set for the authentication information to be sent.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

split *splitchart*: Specifies a separator. It can be a letter, a digit, or a sign such as a percent sign (%) or a pound sign (#).

Usage guidelines

If IMSI/SN binding authentication is enabled, the IMSI/SN information is included in the authentication information in addition to the username. You need to configure a separator to separate different types of information. For example, if you specify the separator as #, the authentication information will be sent in the following format: *imsiinfo#sninfo#username*.

Examples

# Configure the pound sign (#) as the separator for the authentication information to be sent.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] attach-format imsi-sn split #
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for a 4G dial-up profile.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode { **pap** | **chap**| **pap-chap** } **user** *user-name* **password** { **cipher** | **simple** } *password*

undo authentication-mode

Default

No authentication mode is configured for a 4G dial-up profile.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

chap: Specifies CHAP authentication.

pap: Specifies PAP authentication.

pap-chap: Specifies CHAP or PAP authentication.

user *username*: Specifies the username for authentication, a case-sensitive string of 1 to 32 characters.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

password: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters

Examples

# Specify the CHAP authentication mode for the 4G dial-up profile **test**. Specify the CHAP authentication username as **user1** and the password as **123456**.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] authentication-mode chap user user1 password simple 123456
```

New feature: Media Stream Control (MSC) logging

This feature enables the router to generate MSC logs and send the logs to the information center.

Command reference

New command: sip log enable

Use **sip log enable** to enable Media Stream Control (MSC) logging.

Use **undo sip log enable** to disable MSC logging.

Syntax

sip log enable

undo sip log enable

Default

MSC logging is disabled.

Views

Voice view

Predefined user roles

network-admin

Usage guidelines

This command enables the router to generate MSC logs and send the logs to the information center. The information center outputs the logs to a destination according to an output rule. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

MSC logging is used for auditing purposes.

Examples

# Enable MSC logging.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip log enable
```

New feature: IMSI/SN binding authentication

This feature enables the device to include the IMSI/SN information in the LCP authentication information.

Command reference

ppp lcp imsi accept

Use **ppp lcp imsi accept** to enable the client to accept the IMSI binding authentication requests from the LNS.

Use **undo ppp lcp imsi accept** to restore the default.

Syntax

ppp lcp imsi accept

undo ppp lcp imsi accept

Default

The client declines the IMSI binding authentication requests from the LNS.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the client to accept the IMSI binding authentication requests from the LNS.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi accept
```

ppp lcp imsi request

Use **ppp lcp imsi request** to enable the LNS to initiate IMSI binding authentication requests.

Use **undo ppp lcp imsi request** to restore the default.

Syntax

ppp lcp imsi request

undo ppp lcp imsi request

Default

The LNS does not initiate IMSI binding authentication requests.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the LNS to initiate IMSI binding authentication requests.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi request
```

ppp lcp imsi string

Use **ppp lcp imsi string** *imsi-info* to configure the IMSI information on the client.

Use **undo ppp lcp imsi string** to delete the IMSI information on the client.

Syntax

ppp lcp imsi string *imsi-info*

undo ppp lcp imsi string

Default

The client automatically obtains the IMSI information from its SIM card.

Views

Interface view

Predefined user roles

network-admin

Parameters

imsi-info: Specifies the IMSI information, a case-sensitive string of 1 to 31 characters.

Examples

# Configure the IMSI information as **imsi1**.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi string imsi1
```

ppp lcp sn accept

Use **ppp lcp sn accept** to enable the client to accept the SN binding authentication requests from the LNS.

Use **undo ppp lcp sn accept** to restore the default.

Syntax

ppp lcp sn accept

undo ppp lcp sn accept

Default

The client declines the SN binding authentication requests from the LNS.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the client to accept the SN binding authentication requests from the LNS.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp sn accept
```

ppp lcp sn request

Use **ppp lcp sn request** to enable the LNS to initiate SN binding authentication requests.

Use **undo ppp lcp sn request** to restore the default.

Syntax

ppp lcp sn request

undo ppp lcp sn request

Default

The LNS does not initiate SN binding authentication requests.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the LNS to initiate SN binding authentication requests.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi request
```

ppp lcp sn string

Use **ppp lcp sn string** *sn-info* to configure the SN information on the client.

Use **undo ppp lcp sn string** to delete the SN information on the client.

Syntax

ppp lcp sn string *sn-info*

undo ppp lcp sn string

Default

The client automatically obtains the SN information from its SIM card.

Views

Interface view

Predefined user roles

network-admin

Parameters

sn-info: Specifies the SN information, a case-sensitive string of 1 to 31 characters.

Examples

# Configure the SN information as **sn1**.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp sn string sn1
```

ppp user accept-format imsi-sn split

Use **ppp user accept-format imsi-sn split** *splitchart* to configure the separator for the received authentication information.

Use **undo ppp user accept-format** to restore the default.

Syntax

ppp user accept-format imsi-sn split *splitchart*

undo ppp user accept-format

Default

No separator is configured for the received authentication information.

Views

Interface view

Predefined user roles

network-admin

Parameters

splitchart: Specifies the separator. The separator contains one character, and it can be a letter, a digit, or any sign other than the at sign (@), slash (/), and backslash (\).

Usage guidelines

By default, the authentication information contains only the client username. If you include the IMSI or SN information in the authentication information, you need to configure the separator to separate different types of information.

If no IMSI/SN information is received from the peer during the authentication process, the IMSI/SN information split from the received authentication information is used.

Examples

# Configure the pound sign (#) as the separator for the authentication information.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user accept-format imsi-sn split #
```

ppp user attach-format imsi-sn split

Use **ppp user attach-format imsi-sn split** *splitchart* to configure the separator for the sent authentication information.

Use **undo ppp user attach-format** to restore the default.

Syntax

ppp user attach-format imsi-sn split *splitchart*

undo ppp user attach-format

Default

No separator is configured for the sent authentication information.

Views

Interface view

Predefined user roles

network-admin

Parameters

splitchart: Specifies the separator. The separator contains one character, and it can be a letter, a digit, or any sign other than the at sign (@), slash (/), and backslash (\).

Usage guidelines

By default, the authentication information contains only the client username. If you include the IMSI or SN information in the authentication information, you need to configure the separator to separate different types of information.

Examples

# Configure the pound sign (#) as the separator for the sent authentication information.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user attach-format imsi-sn split #
```

ppp user replace

Use **ppp user replace** to replace the client username with the IMSI or SN information for authentication.

Use **undo ppp user replace** to restore the default.

Syntax

ppp user replace { imsi | sn }

undo ppp user replace

Default

The client username is used for authentication.

Views

Interface view

Predefined user roles

network-admin

Examples

# Replace the client username with the IMSI information for authentication.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user replace imsi
```

New feature: Specifying a band for a 4G modem

You can specify a band for a 4G modem.

Command reference

lte band

Use **ite band** to specify a band for a 4G modem.

Use **undo lte band** to restore the default.

Syntax

lte band *band-number*

undo lte band

Default

The default setting varies by 4G modem model.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

band-number: Specifies a band for a 4G modem. The available bands vary by modem model.

Usage guidelines

This command is supported only on the following 4G modems:

- Sierra MC7354 and MC7304.
- Long Sung U8300C, U8300W, and U8300.
- WNC DM11-2.

Examples

# Specify band 3 for Cellular 1/0.

```
<Sysname> system-view
[Sysname] controller cellular 1/0
[Sysname-Controller-Cellular1/0]lte band 3
```

New feature: Using tunnel interfaces as OpenFlow ports

The MSR 2600 routers support using tunnel interfaces as OpenFlow ports.

New feature: NETCONF support for ACL filtering

Support of NETCONF for ACL filtering was added.

Command reference

netconf soap http acl

Use **netconf soap http acl** to apply an ACL to NETCONF over SOAP over HTTP traffic.

Use **undo netconf soap http acl** to restore the default.

Syntax

netconf soap http acl { *acl-number* **|** **name** *acl-name* }

undo netconf soap http acl

Default

No ACL is applied to NETCONF over SOAP over HTTP traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**. The specified ACL must be an existing IPv4 basic ACL.

Usage guidelines

This command is not available in FIPS mode.

Only NETCONF clients permitted by the ACL can access the device through SOAP over HTTP.

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

Examples

# Use ACL 2001 to allow only NETCONF clients in subnet 10.10.0.0/16 to access the device through SOAP over HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
```

```
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

netconf soap https acl

Use **netconf soap https acl** to apply an ACL to NETCONF over SOAP over HTTPS traffic.

Use **undo netconf soap https acl** to restore the default.

Syntax

netconf soap https acl { *acl-number* **|** **name** *acl-name* }

undo netconf soap https acl

Default

No ACL is applied to NETCONF over SOAP over HTTPS traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**. The specified ACL must be an existing IPv4 basic ACL.

Usage guidelines

Only NETCONF clients permitted by the ACL can access the device through SOAP over HTTPS.

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

Examples

# Use ACL 2001 to allow only NETCONF clients in subnet 10.10.0.0/16 to access the device through SOAP over HTTPS.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap https acl 2001
```

New feature: WAAS

Configuring WAAS

This release added support for the Wide Area Application Services (WAAS) feature in the DATA image on the following router series:

- MSR 800.
- MSR 2600.
- MSR 3600.
- MSR 5600.

Command reference

All commands were newly added.

For more information about the commands, see WAAS commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Support for the MKI field in SRTP or SRTCP packets

This feature enables the router to add the MKI field to outgoing SRTP or SRTCP packets. You can set the length of the MKI field.

Command reference

New command: mki

Use **mki** to add the MKI field to outgoing SRTP or SRTCP packets and set the length of the MKI field.

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

Syntax

mki *mki-length*

undo mki

Default

Outgoing SRTP or SRTCP packets do not carry the MKI field.

Views

SIP view

Predefined user roles

network-admin

Parameters

mki-length: Specifies the length of the MKI field, in the range of 1 to 128 bytes.

Usage guidelines

This command takes effect only when SRTP is the media stream protocol for SIP calls. To specify SRTP as the medial stream protocol for SIP calls, use the **srtp** command.

Examples

# Add the MKI field to outgoing SRTP or SRTCP packets and set the length of the MKI field to 1 bit.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] mki 1
```

New feature: SIP domain name

This feature enables the router to populate the CONTACT header field of outgoing SIP packets with the router's SIP domain name.

Command reference

New command: sip-domain

Use **sip-domain** to populate the CONTACT header field of outgoing SIP packets with the router's SIP domain name.

Use **undo sip-domain** to restore the default.

Syntax

sip-domain *domain-name*

undo sip-domain

Default

The router populates the CONTACT header field of an outgoing SIP packet with the IP address of the outgoing interface.

Views

SIP view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the SIP domain name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, underscore (_), hyphen (-), and dot (.).

Examples

# Populate the CONTACT header field of outgoing SIP packets with the SIP domain name **abc.com**.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-domain abc.com
```

New feature: Setting the maximum size of advertisement files

You can set the maximum size of advertisement files sent to wireless clients to 10 MB when the clients access the wireless network.

New feature: Support of VCF for NETCONF

Support for NETCONF was added to VCF.

New feature: Support of SNMP for NETCONF

Support for NETCONF was added to SNMP.

New feature: Support of file system for NETCONF

Support for NETCONF was added to file system.

New feature: Support of PoE for NETCONF

Support for NETCONF was added to PoE.

New feature: Support of RMON for NETCONF

Support for NETCONF was added to RMON.

New feature: Support of policy-based routing for NETCONF

Support for NETCONF was added to policy-based routing.

New feature: Support of BGP for NETCONF

Support for NETCONF was added to BGP.

New feature: Support of OSPF for NETCONF

Support for NETCONF was added to OSPF.

New feature: Support of ping for NETCONF

Support for NETCONF was added to ping.

New feature: Support of tracert for NETCONF

Support for NETCONF was added to tracert.

New feature: Support of L2VPN for NETCONF

Support for NETCONF was added to L2VPN.

New feature: SIP support for VRF

Configuring SIP support for VRF

For information about this feature, see SIP configuration in *H3C MSR Router Series Comware 7 Voice Configuration Guide.*

Command reference

The **vpn-instance** command was added.

For information about the command, see SIP commands in *H3C MSR Router Series Comware 7 Voice Command Reference.*

New feature: IKEv2

Configuring IKEv2

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

For information about the commands, see IPsec commands in *H3C MSR Router Series Comware 7 Command Reference*.

New feature: Specifying an IKEv2 profile for an IPsec policy

Specifying an IKEv2 profile for an IPsec policy

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **ikev2-profile** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Bidirectional BFD control detection for RIP

Configuring bidirectional BFD control detection for RIP

For information about this feature, see RIP configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide.*

Command reference

The **bfd all-interfaces enable**, **rip bfd**, and **rip primary-path-detect bfd** commands were newly added.

For information about the commands, see RIP commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference.*

New feature: OSPF router ID autoconfiguration

Automatically obtaining an OSPF router ID

For information about this feature, see OSPF configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide.*

Command reference

The **display system internal ospf event-log router-id** command was newly added and the **auto-select** keyword was added to the **ospf** command.

For information about the commands, see OSPF commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference* and OSPF probe commands in *H3C MSR Router Series Comware 7 Probe Command Reference*.

New feature: Associating a static route with a track entry

Associating a static route with a track entry

For information about this feature, see static routing configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide.*

Command reference

The **track** keyword was added to the **ip route-static** command.

For information about the command, see static routing commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: VLAN tag processing rule for incoming traffic

Configuring the VLAN tag processing rule for incoming traffic

For information about this feature, see *H3C MSR Router Series Comware 7 VXLAN Configuration Guide*.

Command reference

The **l2vpn rewrite inbound tag** command was added. For information about this command, see *H3C MSR Router Series Comware 7 VXLAN Command Reference*.

New feature: IP-based portal-free rule

Configuring an IP-based portal free-rule

For information about this feature, see portal authentication configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The portal free-rule command was added.

For information about the command, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Portal redirect packet statistics

Displaying/maintaining portal redirect packet statistics

For information about this feature, see portal authentication configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **display portal redirect statistics** and **reset portal redirect statistics** commands were added.

For information about the commands, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: GDVPN

Configuring GDVPN

For information about this feature, see group domain VPN configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

For information about the commands, see group domain VPN commands in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

New feature: OpenFlow instance

Configuring the OpenFlow instance mode

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **port** keyword was added to the **classification** command.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

Binding an OpenFlow instance to ports

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **port** command was added.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

Binding an port to an OpenFlow instance

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **openflow-instance** command was added.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set

Enabling ESN for an IPsec transform set

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **esn enable** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy

Enabling TFC padding for an IPsec policy

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **tfc enable** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: SIP session refresh

Enabling SIP session refresh

In this release, you can enable SIP session refresh for a VoIP voice entity.

Command reference

New command: voice-class sip session refresh

Use **voice-class sip session refresh** to enable SIP session refresh for a VoIP entity.

Use **undo voice-class sip session refresh** to disable SIP session refresh for a VoIP entity.

Syntax

voice-class sip session refresh [**global**]

undo voice-class sip session refresh

Default

A VoIP entity uses the global configuration for SIP session refresh.

Views

VoIP entity view

Predefined user roles

network-admin

Parameters

global: Applies the global configuration for SIP session refresh to the VoIP entity.

Usage guidelines

The configuration for SIP session refresh in VoIP entity view takes priority over that in SIP view.

Examples

# Enable SIP session refresh for VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip session refresh
```

# Apply the global configuration for SIP session refresh to VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip session refresh global
```

Modified feature: User profile

Feature change description

This release added support for QoS policy configuration in user profile view.

Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes

1. Feature change description

This release added support for the IPsec tunnel mode and VXLAN tunnel mode on a tunnel interface.

2. Command changes

1. Modified command: interface tunnel

Old syntax

interface tunnel *number* [**mode** { **advpn** { **gre** | **udp** } [**ipv6**] | **ds-lite-aftr** | **evi** | **gre** [**ipv6**] | **ipv4-ipv4** | **ipv6** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **mpls-te** | **nve** }]

New syntax

interface tunnel *number* [**mode** { **advpn** { **gre** | **udp** } [**ipv6**] | **ds-lite-aftr** | **evi** | **gre** [**ipv6**] | **ipsec** [**ipv6**] | **ipv4-ipv4** | **ipv6** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **mpls-te** | **nve** |**vxlan** }]

Views

System view

Change description

The following parameters were added to the command:

- **mode ipsec**: Specifies the IPv4 IPsec tunnel mode.
- **mode ipsec ipv6**: Specifies the IPv6 IPsec tunnel mode.
- **mode vxlan**: Specifies the VXLAN tunnel mode.

Modified feature: PKI certificate auto-renewal

Feature change description

Support for certificate auto-renewal was added to PKI.

Command changes

Modified command: certificate request mode

Old syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

New syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string* | **renew-before-expire** *days* [**reuse-public-key**] [**auto-append common-name**]] * | **manual** }

Views

PKI domain view

Change description

The following keywords were added to the command:

- **renew-before-expire** *days*: Configures the system to automatically request a new certificate the specified number of days before the current certificate expires. The value range for the *days* argument is 0 to 365. Value 0 indicates that the request for a new certificate is made when the old certificate expires, which might cause service interruptions.
- **reuse-public-key**: Reuses the key pair in the old certificate for the new certificate. If you do not specify this keyword, the system generates a new key pair for the new certificate. The old key pair is replaced with the new one when the new certificate is received from the CA.
- **auto-append common-name**: Automatically appends random data to the common name of the PKI entity for the new certificate. If you do not specify this keyword, the common name of the PKI entity will be unchanged in the new certificate.

New command: display pki certificate renew-status

Use **display pki certificate renew-status** to display the certificate renewal status for a PKI domain.

Syntax

display pki certificate renew-status [**domain** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in **错误!未找到引用源。**. If you do not specify a domain name, this command displays the certificate renewal status for all PKI domains.

Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Examples

# Display the certificate renewal status for all PKI domains.

```
<Sysname> display pki certificate renew-status
Domain name: domain1
Renew time:  03:12:05 2015/12/07
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2015/05/12
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

The command output indicates that the **reuse-public-key** keyword was not configured for PKI domain **domain1** and a new key pair was created for the new certificate.

# Display the certificate renewal status for PKI domain **domain1**.

```
<Sysname> display pki certificate renew-status domain1
Domain name: domain1
Renew time:  03:12:05 2013/12/07
Renew public key:
  Key type: RSA
  Time when  key pair created: 15:40:48 2013/05/12
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

Command output

Field	Description
Renew time	Time when a new certificate will be requested.
Renew public key	Information about the new key pair created for the certificate.
Key type	Key pair type, which can be RSA, DSA, or ECDSA.
Time when key pair created	Time when the key pair was created.
Key code	Public key data.

Modified feature: Configuring the PKI entity DN

Feature change description

Support for the **subject-dn** command was added to PKI. You can use the command to configure the full subject DN string. Each attribute can be specified multiple times with different values.

Command changes

New command: subject-dn

Use **subject-dn** to configure the DN for a PKI entity.

Use **undo subject-dn** to restore the default.

Syntax

subject-dn *dn-string*

undo subject-dn

Default

No DN is configured for a PKI entity.

Views

PKI entity view

Default command level

network-admin

Parameters

dn-string: Specifies the DN for the PKI entity, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The subject DN string is a sequence of *attribute*=*value* pairs separated by commas. Each attribute can be specified multiple times with different values. Supported DN attributes are:

- **CN**—Common-name.
- **C**—Country code.
- **L**—Locality.
- **O**—Organization.
- **OU**—Organization unit.
- **ST**—State or province.

After this command is configured, the following commands do not take effect:

- **common-name**
- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

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

Examples

# Configure the DN for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] subject-dn
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

Modified feature: ADVPN

Feature change description

In this release, you can configure ADVPN group names and ADVPN group-to-QoS policy mappings.

Command changes

New command: advpn group

Use **advpn group** to configure an ADVPN group name.

Use **undo advpn group** to restore the default.

Syntax

advpn group *group-name*

undo advpn group

Default

No ADVPN group name is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

Usage guidelines

This command must be configured on the tunnel interface of a spoke. The spoke sends the ADVPN group name in a hub-spoke tunnel establishment request to a hub. The hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel. If no match is found, the hub does not apply a QoS policy to the hub-spoke tunnel.

If you modify the ADVPN group name after the tunnel is established, the spoke will inform the hub of the modification. The hub will look for an ADVPN group-to-QoS policy mapping that matches the new ADVPN group name and apply the QoS policy in the new mapping.

As a best practice, do not configure an ADVPN group name and apply a QoS policy on the same tunnel interface.

Examples

# Configure **aaa** as the ADVPN group name.

```
<Sysname> system-view
[Sysname] interface tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn group aaa
```

2. New command: advpn map group

Use **advpn map group** to configure a mapping between an ADVPN group and a QoS policy.

Use **undo advpn map group** to delete a mapping between an ADVPN group and a QoS policy.

Syntax

advpn map group *group-name* **qos-policy** *policy-name* **outbound**

undo advpn map group *group-name*

Default

No ADVPN group-to-QoS policy mappings are configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

qos-policy *policy-name*: Specifies the QoS policy name, a case-sensitive string of 1 to 31 characters.

outbound: Applies the QoS policy to the outbound direction.

Usage guidelines

This command must be configured on the tunnel interface of a hub. After receiving a hub-spoke tunnel establishment request from a spoke, the hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name carried in the request. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel.

You can configure multiple ADVPN group-to-QoS policy mappings on a tunnel interface.

You can map multiple ADVPN groups to a QoS policy. You can map an ADVPN group to only one QoS policy.

As a best practice, do not configure an ADVPN group-to-QoS policy mapping and apply a QoS policy on the same tunnel interface.

Examples

# Configure a mapping between ADVPN group **aaa** and QoS policy **bbb** on **Tunnel1**.

```
<Sysname> system-view
[Sysname] interface Tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn map group aaa qos-policy bbb outbound
```

Modified feature: Telnet redirect

Feature change description

In this release, a Telnet redirect user is authenticated by using the authentication settings for the TTY line. The device displays only Telnet redirect authentication information and the authentication result. It does not display the copyright statement.

Support for Telnet redirect authentication was removed from MSR56 routers.

Modified feature: DHCP snooping performance optimization

Feature change description

On a Layer 3 physical interface without subinterface, link aggregation, or snooping configured, the **dhcp snooping enable** command was optimized to cause only a slight impact on receiving non-DHCP packets. If you configure other services on the interface, the performance varies with the services you configure.

Modified feature: OSPF performance optimization

Feature change description

You can set a fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

The value range for the LSU packet sending interval was changed to 0 to 1000 milliseconds.

Command changes

Modified command: spf-schedule-interval

Old syntax

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

New syntax

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

Views

OSPF view

Change description

The *millisecond interval* argument was added to the command. You can specify this argument to set a fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

Modified command: transmit-pacing

Syntax

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

Views

OSPF view

Change description

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

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

Modified feature: IP performance optimization

Feature change description

The device supports recording MAC addresses in TCP packets. You can also configure the device to record the MAC address of the local device in TCP packets.

Command changes

New command: tcp mac-record enable

Use **tcp mac-record enable** to enable MAC address recording in TCP packets.

Use **undo tcp mac-record enable** to disable MAC address recording in TCP packets.

Syntax

tcp mac-record enable

undo tcp mac-record enable

Default

MAC address recording in TCP packets is disabled.

Views

Interface view

Default command level

network-admin

Usage guidelines

This feature records the MAC address of the packet originator in a TCP option. When an attack occurs, the administrator can quickly locate the attack source according to the recorded MAC addresses.

Examples

# Enable MAC address recording in TCP packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 0/1
[Sysname-GigabitEthernet0/1] tcp mac-record enable
```

New command: tcp mac-record local

Use **tcp mac-record local** to record the MAC address of the local device in TCP packets.

Use **undo tcp mac-record local** to restore the default.

Syntax

tcp mac-record local *mac-address*

undo tcp mac-record local

Default

The destination MAC address is recorded.

Views

System view

Default command level

network-admin

Parameters

mac-address: Specifies the MAC address of the local device. The MAC address cannot be all 0s, broadcast MAC address, or multicast MAC address.

Usage guidelines

To make this command take effect, you must enable MAC address recording in TCP packets by using the **tcp mac-record enable** command.

Examples

# Record the MAC address of the local device 0605-0403-0201 in TCP packets.

```
<Sysname> system-view
[Sysname] tcp mac-record local 0605-0403-0201
```

Modified feature: AAA

Feature change description

Starting from this software version, you can configure the authorization method for IKE extended authentication.

Command changes

New command: authorization ike

Use **authorization ike** to configure the authorization method for IKE extended authentication.

Use **undo authorization ike** to restore the default.

Syntax

In non-FIPS mode:

authorization ike { **local** [**none**] **| none | radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization ike

In FIPS mode:

authorization ike { **local | radius-scheme** *radius-scheme-name* [**local**] }

undo authorization ike

Default

The default authorization method for the ISP domain is used for IKE extended authentication.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

# In ISP domain **test**, perform local authorization for IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ike local
```

# In ISP domain **test**, use RADIUS scheme **rd** as the primary authorization method and local authorization as the backup authorization method for IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ike radius-scheme rd local
```

Modified feature: Configuring a cellular interface for a 3G/4G modem

Feature change description

In this release, you can set the RSSI thresholds for a 3G/4G modem.

Command changes

New command: rssi

Use **rssi** to set the RSSI thresholds for a 3G/4G modem.

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

Syntax

rssi { **1xrtt** | **evdo** | **gsm** | **lte** } { **low** *lowthreshold* | **medium** *mediumthreshold* } *

undo rssi { **1xrtt** | **evdo** | **gsm** | **lte** } [**low** | **medium**]

Default

The lower and upper thresholds for a 3G/4G modem are –150 dBm and 0 dBm, respectively.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

1xrtt: Specifies the 1xRTT mode.

evdo: Specifies the EVDO mode.

gsm: Specifies the GSM mode.

lte: Specifies the LTE mode.

low *lowthreshold*: Specifies the lower RSSI threshold value in the range of 0 to 150, which represent a lower RSSI threshold in the range of –150 dBm to 0 dBm. The value of *lowthreshold* cannot be smaller than the value of *mediumthreshold* because the system automatically adds a negative sign to the RSSI thresholds.

medium *mediumthreshold*: Specifies the upper RSSI threshold value in the range of 0 to 150, which represent an upper RSSI threshold in the range of –150 dBm to 0 dBm.

Usage guidelines

The device performs the following operations based on the actual RSSI of the 3G/4G modem:

- Sends a trap that indicates high RSSI when the RSSI exceeds the upper threshold.
- Sends a trap that indicates normal RSSI when the RSSI is between the lower threshold and upper threshold (included).
- Sends a trap that indicates low RSSI when the RSSI drops to or below the lower threshold.
- Sends a trap that indicates low RSSI every 10 minutes when the RSSI remains equal to or smaller than the lower threshold.

To view the RSSI change information for a 3G/4G modem, use the **display cellular** command.

Examples

# Set the lower threshold for a 3G/4G modem in GSM mode to –110 dBm.

```
<Sysname> system-view
[Sysname] interface cellular 0/0
[Sysname-Cellular0/0] rssi gsm low 110
```

Modified feature: QoS on VXLAN tunnel interfaces

Feature change description

This software version added support for QoS in the outbound direction of VXLAN tunnel interfaces.

Command changes

None.

Modified feature: Option 60 encapsulation in DHCP replies

Feature change description

Disabling Option 60 encapsulation in DHCP replies.

Modified feature: MPLS QoS support for matching the EXP field

Feature change description

In this release, MPLS QoS supports matching the EXP fields in both the topmost (first) MPLS label and the second MPLS label.

Command changes

New command: 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
```

Modified feature: MPLS QoS support for marking the EXP field

Feature change description

In this release, MPLS QoS supports marking the EXP fields in both the topmost (first) MPLS label and the second MPLS label.

Command changes

New command: 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 *second-mpls-exp-value*

undo remark second-mpls-exp *second-mpls-exp-value*

Default

No EXP value marking action for the second MPLS label is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

second-mpls-exp-value: Specifies an EXP value for the second MPLS label, in the range of 0 to 7.

Examples

# Define a traffic behavior to mark packets with EXP value 3 for the second MPLS label.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark second-mpls-exp 3
```

Modified feature: Automatic configuration

Feature change description

A limit was added to the number of automatic attempts. After the limit is reached, the automatic configuration process ends.

If you set the limit to 0, only one automatic configuration attempt is allowed.

Modified feature: User profile

Feature change description

In this release, the user profile name supports using dots (.).

Command change

Modified command: user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

Views

System view

Change description

Before modification: The user profile name is a case-sensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_), and the name must start with an English letter.

After modification: The user profile name is a case-sensitive string of 1 to 31 characters. Valid characters are letters, digits, underscores (_), and dots (.), and the name must start with an English letter.

Modified feature: Default size of the TCP receive and send buffer

Feature change description

The default value for the TCP receive and send buffer size was changed to 63 KB.

Command changes

Modified command: tcp window

Syntax

tcp window *window-size*

undo tcp window

Views

System view

Change description

Before modification: The default value for the *window-size* argument was 64 KB.

After modification: The default value for the *window-size* argument is 63 KB.

Modified feature: Support for per-packet load sharing

Feature change description

The **per-packet** keyword was added to the **ip load-sharing mode** command to support per-packet load sharing.

Command changes

Modified command: ip load-sharing mode

Old syntax

Centralized devices:

ip load-sharing mode per-flow [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *]

Centralized IRF devices–Distributed devices–In standalone mode:

ip load-sharing mode per-flow [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] [**slot** *slot-number*]

Distributed devices–In IRF mode:

ip load-sharing mode per-flow [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] [**chassis** *chassis-number* **slot** *slot-number*]

New syntax

Centralized devices:

ip load-sharing mode { **per-flow** [[**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] | **per-packet** }

Centralized IRF devices–Distributed devices–In standalone mode:

ip load-sharing mode { **per-flow** [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] | **per-packet** }

Distributed devices–In IRF mode:

ip load-sharing mode { **per-flow** [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] | **per-packet** }

Views

System view

Change description

The **per-packet** keyword was added to the **ip load-sharing mode** command to support per-packet load sharing.

Modified feature: Default user role

Feature change description

The default user role can be changed. The *role-name* argument was added to the **role default-role enable** command for specifying a user role as the default user role.

Command changes

Modified command: role default-role enable

Old syntax

role default-role enable

undo role default-role enable

New syntax

role default-role enable [*role-name*]

undo role default-role enable

Views

System view

Change description

Before modification: The default user role is network-operator.

After modification: The *role-name* argument was added to specify any user role that exists in the system as the default user role. The argument is a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the default user role is network-operator.

Modified feature: Debugging

Feature change description

The **all** keyword and the **timeout** *time* option were removed from the **debugging** command. You can no longer use the **debugging all** command to enable debugging for all modules or specify the timeout time for the **debugging all** command.

Command changes

Modified command: debugging

Old syntax

debugging { **all** [**timeout** *time*] **|** *module-name* [*option*] }

undo debugging { **all** **|** *module-name* [*option*] }

New syntax

debugging *module-name* [*option*]

undo debugging *module-name* [*option*]

Views

User view

Change description

The following parameters were removed from the **debugging** command:

- **all**: Enables debugging for all modules.

timeout *time*: Specifies the timeout time for the **debugging all** command. The system automatically executes the **undo debugging all** command after the timeout time. The *time* argument is in the range of 1 to 1440 minutes. If you do not specify a timeout time, you must manually execute the **undo debugging all** command to disable debugging for all modules.

Modified feature: SSH username

Feature change description

In this release, an SSH username cannot be **a**, **al**, **all**, or include the following characters: \ | / : * ? < >

The at sign (@) can only be used in the username format *pureusername@domain* when the username contains an ISP domain name.

Command changes

Modified command: ssh user

Syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *domain-name* **|** **publickey** *keyname* } }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey assign** { **pki-domain** *domain-name* **|** **publickey** *keyname* } }

undo ssh user *username*

Views

System view

Change description

Before modification: The *username* argument is a case-insensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the format *pureusername@domain*.

After modification: The *username* argument is a case-insensitive string of 1 to 80 characters, excluding **a**, **al**, **all**, and the following characters:
\ | / : * ? < >

The at sign (@) can only be used in the username format *pureusername@domain* when the username contains an ISP domain name. The pure username can contain 1 to 55 characters and the domain name can contain 1 to 24 characters. The whole username cannot exceed 80 characters.

Modified feature: IS-IS hello packet sending interval

Feature change description

The value range of the interval for sending hello packets was changed to 1 to 255 seconds.

Command changes

Modified command: isis timer hello

Syntax

isis timer hello *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

Views

Interface view

Change description

The value range for the *seconds* argument was changed to 1 to 255 seconds.

Modified feature: 802.1X redirect URL

Feature change description

The value range for the *url-string* argument was changed to 1 to 256 characters for the **dot1x ead-assistant url** command.

Command changes

Modified command: dot1x ead-assistant url

Syntax

dot1x ead-assistant url *url-string*

Views

System view

Change description

Before modification: The value range for the *url-string* argument is 1 to 64 characters.

After modification: The value range for the *url-string* argument is 1 to 256 characters.

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Feature change description

You can specify a source interface for tracing NTP servers from the reference source to the primary NTP server.

Command changes

Modified command: display ntp-service trace

Old syntax

display ntp-service trace

New syntax

display ntp-service trace [**source** *interface-type interface-number*]

Views

Any view

Change description

The **source** *interface-type interface-number* option was added to the **display ntp-service trace** command.

Modified feature: Saving, rolling back, and loading the configuration

The following configuration guidelines were added when you use NETCONF to save, roll back, or load the configuration:

- The save, rollback, and load operations supplement NETCONF requests. Performing the operations might consume a lot of system resources.
- Do not perform the save, rollback, or load operation when another user is performing the operation. If multiple users simultaneously perform the save, rollback, or load operation, the result returned to each user might be inconsistent with the user request.

Modified feature: Displaying information about SSH users

Feature change description

In this release, the **display ssh user-information** command does not display the public key name for an SSH user that uses password authentication.

Command changes

Modified command: display ssh user-information

Syntax

display ssh user-information [*username*]

Views

Any view

Change description

Before modification: The **User-public-key-name** field in the command output displays **null** for an SSH user that uses password authentication.

After modification: The **User-public-key-name** field in the command output is blank for an SSH user that uses password authentication.

Modified feature: SIP trusted nodes

Configuring SIP trusted nodes

In this release, you can enable the trusted node feature by using the **ip address trusted authenticate** command. You also can display information about SIP trusted nodes by using the **display voice ip address trusted list** command.

Command changes

The **display voice ip address trusted list** and **ip address trusted authenticate** commands were added.

New command: display voice ip address trusted list

Use **display voice ip address trusted list** to display information about trusted nodes.

Syntax

display voice ip address trusted list

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays trusted nodes in the trusted node list and call destination IP addresses.

Examples

# Display information about trusted nodes.

```
<Sysname> display voice ip address trusted list
IP address trusted authentication: Enabled

VoIP entity IP addresses:
Entity tag      State    SIP IP address
----------      -----    --------------
20              Up       192.168.4.110
53232           Down     192.168.4.210
55555           Up       192.168.4.210
9613            Up       192.168.4.125

IP address trusted list:
 192.168.4.0 255.255.255.0
 192.168.5.120 255.255.255.255
```

Command output

Field	Description
IP address trusted authentication	Whether IP address trusted authentication is enabled: • Enabled. • Disabled.
VoIP entity IP addresses	Trusted IP addresses for VoIP entities.
Entity tag	Tag of a VoIP entity.
State	Status of a VoIP entity: • Up. • Down.
SIP IP address	Call destination IP address of a VoIP entity.
IP address trusted list	List of trusted nodes.

New command: ip address trusted authenticate

Use **ip address trusted authenticate** to enable IP address trusted authentication.

Use **undo ip address trusted authenticate** to disable IP address trusted authentication.

Syntax

ip address trusted authenticate

undo ip address trusted authenticate

Default

IP address trusted authentication is disabled. All nodes are regarded as trusted, and the device accepts calls from any nodes.

Views

SIP view

Predefined user roles

network-admin

Usage guidelines

After you enable this feature, the device accepts calls only from trusted nodes.

For calls to be successfully established, configure the proxy server, registrars, the DNS server, and the MWI server as trusted nodes.

Examples

# Enable IP address trusted authentication.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
```

```
[Sysname-voice-sip] ip address trusted authenticate
```

Modified feature: IPsec ESP encryption algorithms

Feature change description

Support for the following IPsec ESP encryption algorithms was added in high encryption mode:

- AES algorithm in CTR mode.
- Camellia algorithm in CBC mode.
- GMAC algorithm.
- GCM algorithm.
- SM1 algorithm in CBC mode.
- SM4 algorithm.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following arguments were added to the **esp encryption-algorithm** command:

- *aes-ctr-128.*
- *aes-ctr-192.*
- *aes-ctr-256.*
- *camellia-cbc-128.*
- *camellia-cbc-192.*
- *camellia-cbc-256.*
- *gmac-128.*
- *gmac-192.*
- *gmac-256.*
- *gcm-128.*
- *gcm-192.*
- *gcm-256.*
- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*

- *sm4-cbc.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: IPsec ESP authentication algorithms

Feature change description

Support for the following IPsec ESP authentication algorithms was added:

- AES-XCBC-MAC.
- HMAC-SHA-25.
- HMAC-SHA-384.
- HMAC-SHA-512.
- HMAC-SM3.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following arguments were added to the **esp authentication-algorithm** command:

- *aes-xcbc-mac.*
- *sha256.*
- *sha384.*
- *sha512.*
- *sm3.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: IPsec AH authentication algorithms

Feature change description

Support for the following IPsec AH authentication algorithms was added:

- AES-XCBC-MAC.
- HMAC-SHA-256.
- HMAC-SHA-384.
- HMAC-SHA-512.
- HMAC-SM3.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following arguments were added to the **ah authentication-algorithm** command:

- *aes-xcbc-mac.*
- *sha256.*
- *sha384.*
- *sha512.*
- *sm3.*

For more information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Specifying an encryption algorithm for an IKE proposal

Feature change description

In this release, you can specify the following encryption algorithms for an IKE proposal:

- *sm1-cbc-128.*
- *sm1-cbc-192.*

- *sm1-cbc-256.*

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following keywords were added to the **encryption-algorithm** command:

- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Specifying an authentication algorithm for an IKE proposal

Feature change description

In this release, you can specify the *sm3* authentication algorithm for an IKE proposal.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The *sm3* argument was added to the **authentication-algorithm** command.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Generating asymmetric key pairs

Feature change description

In this release, you can generate ECDSA key pairs by using the secp384r1 elliptic curve.

For information about this feature, see public key management in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The **secp384r1** keyword was added to the **public-key local create** command.

For information about the command, see public key management commands in *H3C MSR Router Series Comware 7 Command Reference*.

Modified feature: Specifying an ECDSA key pair for certificate request

Feature change description

In this release, you can specify an ECDSA key pair with a specific key length for certificate request. Supported key lengths are:

- 192 bits.
- 256 bits.
- 384 bits.

For information about this feature, see PKI in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following keywords were added to the **public-key ecdsa name** command:

- **secp192r1**.
- **secp256r1**.
- **secp384r1**.

For information about the command, see PKI commands in *H3C MSR Router Series Comware 7 Command Reference*.

Modified feature: QoS MIB

Feature change description

In this release, QoS MIB information changed.

Modified feature: Enabling PFS for an IPsec transform set

Feature change description

In this release, you can enable PFS using 256-bit or 384-bit ECP Diffie-Hellman group for an IPsec transform set.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The **dh-group19** and **dh-group20** keywords were added to the **pfs** command.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Displaying track entry infomration

Feature change description

The following fields were added to the output of the **display track** command:

- IP route.
- VPN instance name.
- Protocol.

- Nexthop interface.

Command changes

Modified command: display track

Syntax

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

Views

Any view

Change description

The following fields were added to the command output:

- IP route.
- VPN instance name.
- Protocol.
- Nexthop interface.

Removed feature: Tiny proxy

Feature change description

The tiny proxy feature was removed.

Removed command

http-proxy

Syntax

http-proxy

undo http-proxy

Views

System view

Removed feature: Displaying switching fabric channel usage

Feature change description

Support for displaying switching fabric channel usage on interface cards was removed.

Removed command

display fabric utilization

Syntax

In standalone mode:

display fabric utilization [**slot** *slot-number*]

In IRF mode:

display fabric utilization [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Release 0408P05

This release has the following changes:

New feature: BGP trap support for VRF information

New feature: SSH redirect

New feature: BGP trap support for VRF information

VRF information is added to BGP traps as the context name.

New feature: SSH redirect

Configuring SSH redirect

About SSH redirect

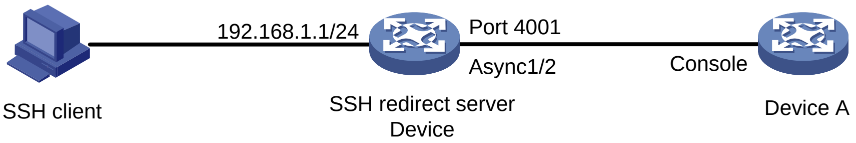
SSH redirect provides redirect service for Stelnet clients. An Stelnet client can access a destination device by using the IP address of the SSH redirect server instead of the IP address of the destination device.

As shown in Figure 1, a user can log in to the SSH redirect server (Device) through Stelnet, and then access the destination device (Device A).

To access Device A, perform the following tasks on the PC:

1. Launch an SSH client software on the PC to establish a connection.
2. Configure connection parameters according to the authentication method.
3. Enter IP address 192.168.1.1 and listening port 4001 of the SSH redirect server.
4. When the login prompt appears on the PC, press **Enter** to enter user view of Device A.

Figure 1 Logging in to Device A through the SSH redirect server



Restrictions and guidelines

The device (SSH redirect server) allows only one login to the same destination device at a time.

Prerequisites

Before you configure SSH redirect, complete the following tasks:

- Use an asynchronous interface of the SSH redirect server to connect to the console port or AUX port of the destination device. An asynchronous interface can be a dedicated asynchronous interface or a synchronous/asynchronous serial interface operating in asynchronous mode.
- If the SSH redirect server is connected to the AUX port of the destination device, perform the following tasks:
  a. Log in to the destination device through the console port.
  b. Disable login authentication for the AUX line.

Procedure

Configuring the asynchronous serial interface

Step	Command	Remarks
54. Enter system view.	**system-view**	N/A
55. Enter synchronous/asynchronous serial interface view or asynchronous interface view.	- Enter synchronous/asynchronous serial interface view and configure it to operate in asynchronous mode: **a. interface serial** *interface-number* **b. physical-mode async** - Enter asynchronous interface view: **interface async** *interface-number*	To use a synchronous/asynchronous serial interface, you must use a connector to connect the interface to the destination device.
56. Set the operating mode to flow mode.	**async-mode flow**	By default, an asynchronous serial interface operates in protocol mode.
57. (Optional.) Disable level detection.	**undo detect dsr-dtr**	By default, level detection is enabled. Whether this command is required depends on the destination device.
58. Return to system view.	**quit**	N/A

Configuring the AUX/TTY user line

Step	Command	Remarks
59. Enter AUX or TTY line view.	**line** { *first-number1* [*last-number1*] | { **aux** | **tty** } *first-number2* [*last-number2*] }	N/A
60. (Optional.) Enable the terminal service.	**shell**	By default, the terminal service is enabled on all user lines.
61. Set the transmission rate.	**speed** *speed-value*	By default, the transmission rate is 9600 bps. The user line must use the same transmission rate as the destination device.
62. Enable stop bit setting consistency detection.	**stopbit-error intolerance**	By default, stop bit setting consistency detection is disabled.
63. Specify the number of stop bits.	**stopbits** { **1** | **1.5** | **2** }	By default, the number of stop bits is 1. Set the same number of stop bits for the user line on the SSH redirect server as the destination device.

Configuring SSH redirect

Step	Command	Remarks
64. Enable SSH redirect.	**ssh redirect enable**	By default, SSH redirect is disabled.
65. (Optional.) Specify an SSH redirect listening port.	**ssh redirect listen-port** *port-number*	By default, the listening port number of SSH redirect is the absolute user line number plus 4000.
66. (Optional.) Set the idle-timeout timer for the redirected connection.	**ssh redirect timeout** *time*	The default idle-timeout timer is 360 seconds.
67. (Optional.) Terminate the redirected SSH connection.	**ssh redirect disconnect**	N/A
68. Return to system view.	**quit**	N/A
69. (Optional.) Associate the SSH redirect listening port with an IP address.	**ssh ip alias** *ip-address* *port-number*	By default, an SSH redirect listening port is not associated with an IP address.

Command reference

Modified command: display ssh server

Old syntax

display ssh server { **session** | **status** }

New syntax

Centralized devices:

display ssh server { **session** | **status** }

Distributed devices in standalone mode/centralized devices in IRF mode:

display ssh server { **session** [**slot** *slot-number* [**cpu** *cpu-number*]] | **status** }

Distributed devices in IRF mode:

display ssh server { **session** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] | **status** }

Views

Any view

Command change description

After modification, parameters were added to the command and the parameters available for a device vary by device type.

- **slot** *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays the SSH server sessions for all cards. (Distributed devices in standalone mode.)

- **slot** *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the SSH server sessions for all member devices. (Centralized IRF devices, IRF 3 incapable.)
- **slot** *slot-number*: Specifies an IRF member device by its member ID or specifies a PEX by its virtual slot number. On an IRF 2 fabric, this command displays the SSH server sessions for all member devices if you do not specify a member device. On an IRF 3 system, this command displays the SSH server sessions for all IRF 2 member devices and PEXs if you do not specify an IRF 2 member device or PEX. (Centralized IRF devices, IRF 3 capable.)
- **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. If you do not specify a card, this command displays the SSH server sessions for all cards. (Distributed devices–In IRF mode, IRF 3 incapable.)
- **chassis** *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device or specifies a PEX. The *chassis-number* argument represents the member ID of the IRF member device or the virtual chassis number of the PEX. The *slot-number* argument represents the slot number of the card or PEX. On an IRF 2 fabric, this command displays the SSH server sessions for all member devices if you do not specify a member device. On an IRF 3 system, this command displays the SSH server sessions for all IRF 2 member devices and PEXs if you do not specify a member device or PEX. (Distributed devices–In IRF mode, IRF 3 capable.)
- **cpu** *cpu-number*: Specifies a CPU by its number. This option is available only if multiple CPUs are available on the specified slot.

New command: ssh ip alias

Use **ssh ip alias** to associate an SSH redirect listening port with an IP address.

Use **undo ssh ip alias** to delete the IP address associated with the SSH redirect listening port.

Syntax

ssh ip alias *ip-address port-number*

undo ssh ip alias *ip-address*

Default

An SSH redirect listening port is not associated with an IP address.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address to be associated with the SSH redirect listening port. The IP address cannot be the address of an interface on the device, but can be on the same subnet as the device.

port-number: Specifies an SSH redirect listening port number in the range of 4000 to 50000.

Usage guidelines

The SSH redirect server can provide the SSH redirect service after SSH redirect is enabled and an SSH redirect listening port is configured. The SSH client can use the **ssh2** *ip address port number* command to access the destination device. The *ip address* argument and the *port number* argument specify the IP address of the SSH redirect server and the SSH redirect listening port, respectively.

After the **ssh ip alias** command is configured, the client can use the **ssh2** *ip address* command to access the destination device. The *ip address* argument specifies the IP address associated with the SSH redirect listening port.

If you specify multiple SSH redirect listening ports for an IP address, the most recent configuration takes effect.

Examples

# Associate SSH redirect listening port 2000 with IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] ssh ip alias 1.1.1.1 4000
```

New command: ssh redirect disconnect

Use **ssh redirect disconnect** to terminate the redirected SSH connection.

Syntax

ssh redirect disconnect

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Examples

# Manually terminate the redirected SSH connection on TTY line 1.

```
<Sysname> system-view
[Sysname] line tty 1
[Sysname-line-tty1] ssh redirect disconnect
```

New command: ssh redirect enable

Use **ssh redirect enable** to enable SSH redirect for a user line.

Use **undo ssh redirect enable** to disable SSH redirect for a user line.

Syntax

ssh redirect enable

undo ssh redirect enable

Default

SSH redirect is disabled for a user line.

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Usage guidelines

Configure the user line connected to the destination device to use the same transmission rate and number of stop bits as the destination device. To change the transmission rate for the user line, use the **speed** command.

To identify whether the user line and the destination device are using the same number of stop bits, use the **stopbit-error intolerance** command. To change the number of stop bits, use the **stopbits** command.

For more information about the transmission rate and stop bits, see the login management configuration in *Fundamentals Configuration Guide*.

Examples

# Enable SSH redirect on TTY line 7.

```
<Sysname> system-view
[Sysname] line tty 7
[Sysname-line-tty7] ssh redirect enable
```

New command: ssh redirect listen-port

Use **ssh redirect listen-port** to set a listening port of SSH redirect.

Use **undo ssh redirect listen-port** to restore the default.

Syntax

ssh redirect listen-port *port-number*

undo ssh redirect listen-port

Default

The SSH redirect listening port number is the absolute user line number plus 4000.

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Parameters

port-number: Specifies the number of the SSH redirect listening port, in the range of 4000 to 50000.

Usage guidelines

The device redirects only SSH connection requests destined for the SSH redirect listening port.

Examples

# Set the SSH redirect listening port number to 5000 on TTY line 1.

```
<Sysname> system-view
[Sysname] line tty 1
[Sysname-line-tty1] ssh redirect listen-port 5000
```

New command: ssh redirect timeout

Use **ssh redirect timeout** to set the idle-timeout timer for the redirected SSH connection.

Use **undo ssh redirect timeout** to restore the default.

Syntax

ssh redirect timeout *time*

undo ssh redirect timeout

Default

The idle-timeout timer is 360 seconds.

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Parameters

time: Specifies the idle-timeout timer in seconds. The value range is 0 to 86400. To disable the timeout mechanism, set the timeout timer to 0.

Usage guidelines

If no data is received from the SSH client before the timer expires, the user line terminates the redirected connection.

Examples

# Set the idle-timeout timer to 200 seconds for the redirected SSH connection.

```
<Sysname> system-view
[Sysname] line tty 1
[Sysname-line-tty1] ssh redirect timeout 200
```

Release 0407

None

ESS 0404P06

None

ESS 0403

None

HPE MSR954_MSR954P_MSR958-CMW710-R411 Release Notes

Software Feature Changes

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

Contents

Release 0411

None.

Release 0410

This release has the following changes:

New feature: Support of multicast for ADVPN

New feature: Application layer state filtering

New feature: SIP keepalive

New feature: Multicast fast forwarding

New feature: Attack defense policy application to a security zone

New feature: AAA support for IKE extended authentication

New feature: Percentage-based CAR

New feature: Logging OSPF router ID conflict events

New feature: AFT

New feature: Configuring enhanced CC authentication in FIPS mode

New feature: Support of AAA for NETCONF

New feature: Mobile IP tunnel interface settings

New feature: LISP

New feature: LISP tunnel entries and dynamic mobility

New feature: Support of IPv6 multicast routing for VPN instances

New feature: LISP virtual machine multi-hop mobility and DDT

New feature: LISP NSR

New feature: PPPoE client support for IPv6

New feature: DPI engine and content filtering

New feature: IPS

New feature: NBAR

New feature: URL filtering

New feature: Local portal Web server

New feature: Support of portal for NETCONF

New feature: Newly-added MIB objects

New feature: IPS, ACG, and SSL VPN licenses

New feature: Support of NQA for NETCONF

New feature: Configuring CWMP to support VPN

New feature: Transceiver module source alarm

New feature: VLAN interface performance optimization

New feature: NAT support for multicast source address in PIM join/prune packets

New feature: GDOI GM group anti-replay window

New feature: SIP compatibility

New feature: Voice VLAN

New feature: L2TP-based EAD

New feature: BFD for an aggregation group

New feature: 4G modem IMSI/SN binding authentication

New feature: Media Stream Control (MSC) logging

New feature: IMSI/SN binding authentication

New feature: Specifying a band for a 4G modem

New feature: Using tunnel interfaces as OpenFlow ports

New feature: NETCONF support for ACL filtering

New feature: WAAS

New feature: Support for the MKI field in SRTP or SRTCP packets

New feature: SIP domain name

New feature: Setting the maximum size of advertisement files

New feature: Support of VCF for NETCONF

New feature: Support of SNMP for NETCONF

New feature: Support of file system for NETCONF

New feature: Support of PoE for NETCONF

New feature: Support of RMON for NETCONF

New feature: Support of policy-based routing for NETCONF

New feature: Support of BGP for NETCONF

New feature: Support of OSPF for NETCONF

New feature: Support of ping for NETCONF

New feature: Support of tracert for NETCONF

New feature: Support of L2VPN for NETCONF

New feature: SIP support for VRF

New feature: IKEv2

New feature: Specifying an IKEv2 profile for an IPsec policy

New feature: Bidirectional BFD control detection for RIP

New feature: OSPF router ID autoconfiguration

New feature: Associating a static route with a track entry

New feature: VLAN tag processing rule for incoming traffic

New feature: IP-based portal-free rule

New feature: Portal redirect packet statistics

New feature: GDVPN

New feature: OpenFlow instance

New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set

New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy

New feature: SIP session refresh

Modified feature: User profile

Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes

Modified feature: PKI certificate auto-renewal

Modified feature: Configuring the PKI entity DN

Modified feature: ADVPN

Modified feature: Telnet redirect

Modified feature: DHCP snooping performance optimization

Modified feature: OSPF performance optimization

Modified feature: IP performance optimization

Modified feature: AAA

Modified feature: Configuring a cellular interface for a 3G/4G modem

Modified feature: QoS on VXLAN tunnel interfaces

Modified feature: Option 60 encapsulation in DHCP replies

Modified feature: MPLS QoS support for matching the EXP field

Modified feature: MPLS QoS support for marking the EXP field

Modified feature: Automatic configuration

Modified feature: User profile

Modified feature: Default size of the TCP receive and send buffer

Modified feature: Support for per-packet load sharing

Modified feature: Default user role

Modified feature: Debugging

Modified feature: SSH username

Modified feature: IS-IS hello packet sending interval

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Modified feature: Saving, rolling back, and loading the configuration

Modified feature: Displaying information about SSH users

Modified feature: SIP trusted nodes

Modified feature: IPsec ESP encryption algorithms

Modified feature: IPsec ESP authentication algorithms

Modified feature: IPsec AH authentication algorithms

Modified feature: Specifying an encryption algorithm for an IKE proposal

Modified feature: Specifying an authentication algorithm for an IKE proposal

Modified feature: Generating asymmetric key pairs

Modified feature: Specifying an ECDSA key pair for certificate request

Modified feature: QoS MIB

Modified feature: Enabling PFS for an IPsec transform set

Modified feature: Displaying track entry infomration

Removed feature: Tiny proxy

Removed feature: Displaying switching fabric channel usage

New feature: Support of multicast for ADVPN

Configuring support of multicast for ADVPN

For information about this feature, see IPv4/IPv6 PIM and IPv4/IPv6 multicast routing and forwarding in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide.*

Command reference

The following commands were added:

- **display ipv6 pim nbma-link**.
- **display pim nbma-link**.
- **ipv6 pim nbma-mode**.
- **pim nbma-mode**.

ADVPN multicast parameters were added to the following commands:

- **display ipv6 multicast forwarding df-info**.
- **display ipv6 multicast forwarding-table**.
- **display ipv6 multicast routing-table**.
- **display ipv6 pim df-info**.
- **display ipv6 pim routing-table**.
- **display multicast forwarding df-info**.
- **display multicast forwarding-table**.
- **display multicast routing-table**.
- **display pim df-info**.
- **display pim routing-table**.

For information about the commands, see IPv4/IPv6 PIM and IPv4/IPv6 multicast routing and forwarding commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference.*

New feature: Application layer state filtering

Configuring application layer state filtering

For information about this feature, see ASPF in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following keywords were added to the **detect** command:

- **dns**.
- **http**.
- **smtp**.
- **action**.

- **drop**.

The fields that indicate application layer status were added to the output from the **display aspf policy** command.

For information about the commands, see ASPF in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: SIP keepalive

Configuring SIP keepalive

You can configure in-dialog keepalive and out-of-dialog keepalive.

Command reference

New command: options-ping

Use **options-ping** to globally enable in-dialog keepalive.

Use **undo options-ping** to globally disable in-dialog keepalive.

Syntax

options-ping *seconds*

undo options-ping

Default

In-dialog keepalive is disabled globally.

View

SIP view

Predefined use roles

network-admin

Parameters

seconds: Specifies the global interval for sending OPTIONS messages during a session, in the range of 60 to 1200 seconds.

Usage guidelines

This command enables the device to periodically send OPTIONS messages at the specified interval to monitor the status of the remote SIP UA during a session. It does not take effect when the session refresh negotiation succeeds before a call is established.

If you disable this feature, the device does not send OPTIONS messages after a call is established.

Example

# Globally enable in-dialog keepalive and set the interval to 60 seconds for sending OPTIONS messages during a session.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] options-ping 60
```

New command: voice-class sip options-ping

Use **voice-class sip options-ping** to enable in-dialog keepalive for a VoIP entity.

Use **voice-class sip options-ping** to disable in-dialog keepalive for a VoIP entity.

Syntax

voice-class sip options-ping { **global** | *seconds* }

undo voice-class sip options-ping

Default

A VoIP entity uses the global configuration for in-dialog keepalive.

Views

VoIP entity view

Predefined user roles

network-admin

Parameters

global: Applies the global configuration for in-dialog keepalive to the VoIP entity.

seconds: Specifies the interval for sending OPTIONS messages during a session, in the range of 60 to 1200 seconds.

Usage guidelines

For a VoIP entity, the entity-specific in-dialog keepalive interval takes priority over the global in-dialog keepalive interval set in SIP view.

Examples

# Enable in-dialog keepalive for VoIP entity 1 and set the interval to 60 seconds for sending OPTIONS messages during a session.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip options-ping 60
```

# Apply the global configuration for in-dialog keepalive to VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip options-ping global
```

New feature: Multicast fast forwarding

Configuring multicast fast forwarding

In this release, the router supports multicast fast forwarding.

Command reference

New command: display multicast fast-forwarding cache

Use **display multicast fast-forwarding cache** to display information about multicast fast forwarding entries.

Syntax

Centralized devices:

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* **|** *group-address*] *

Distributed devices in standalone mode:Centralized IRF devices:

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* **|** *group-address*] * [**slot** *slot-number*]

Distributed devices in IRF mode:

display multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*source-address* **|** *group-address*] * [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command displays multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Display multicast fast forwarding entries on the public network.

```
<Sysname> display multicast fast-forwarding cache
Total 1 entries, 1 matched
(60.1.1.200, 225.0.0.2)
Status : Enabled
Source port: 2001 Destination port: 2002
Protocol : 2 Flag : 0x2
Incoming interface: GigabitEthernet1/0/3
```

```
List of 1 outgoing interfaces:
GigabitEthernet1/0/2
Status: Enabled Flag: 0x14
```

Table 1 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the multicast fast forwarding table, and the total number of matching (S, G) entries.
(60.1.1.200, 225.0.0.2)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The interface is added to the entry because of packets passed through between cards. • **0x2**—The interface is added to an existing entry. • **0x4**—The MAC address of the interface is needed for fast forwarding. • **0x8**—The interface is an outgoing interface associated with the incoming VLAN or super VLAN interface. • **0x10**—The interface is associated with the entry. • **0x20**—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • **Enabled**—Available. • **Disabled**—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

New command: reset multicast fast-forwarding cache

Use **reset multicast fast-forwarding cache** to clear multicast fast forwarding entries.

Syntax

Centralized devices:

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** }

Distributed devices in standalone mode:Centralized IRF devices:

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** } [**slot** *slot-number*]

Distributed devices in IRF mode:

reset multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *source-address* | *group-address* } * | **all** } [**chassis** *chassis-number* **slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears multicast fast forwarding entries on the public network.

source-address: Specifies a multicast source address.

group-address: Specifies a multicast group address in the range of 224.0.1.0 to 239.255.255.255.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command clears multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Clear all multicast fast forwarding entries on the public network.

```
<Sysname> reset multicast fast-forwarding cache all
```

# Clear the multicast fast forwarding entry for multicast source and group (20.0.0.2, 225.0.0.2) on the public network.

```
<Sysname> reset multicast fast-forwarding cache 20.0.0.2 225.0.0.2
```

New command: display ipv6 multicast fast-forwarding cache

Use **display ipv6 multicast fast-forwarding cache** to display information about IPv6 multicast fast forwarding entries.

Syntax

Centralized devices:

display ipv6 multicast [vpn-instance *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* **|** *ipv6-group-address*] *

Distributed devices in standalone mode:Centralized IRF devices:

display ipv6 multicast [vpn-instance *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* **|** *ipv6-group-address*] * [**slot** *slot-number*]

Distributed devices in IRF mode:

display ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** [*ipv6-source-address* **|** *ipv6-group-address*] * [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command displays IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers from 0 to F.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays IPv6 multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays IPv6 multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command displays IPv6 multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Display IPv6 multicast fast forwarding entries on the public network.

```
<Sysname> display ipv6 multicast fast-forwarding cache
Total 1 entries, 1 matched

(FE1F:60::200, FF0E::1)
Status     : Enabled
Source port: 2001                   Destination port: 2002
Protocol   : 2                      Flag            : 0x2
Incoming Interfacfe: GigabitEthernet1/0/3
List of 1 outgoing interfaces:
GigabitEthernet1/0/2
Status: Enabled              Flag: 0x14
```

Table 2 Command output

Field	Description
Total 1 entries, 1 matched	Total number of (S, G) entries in the IPv6 multicast fast forwarding table, and the total number of matching (S, G) entries.
(FE1F:60::200, FF0E::1)	(S, G) entry.
Protocol	Protocol number.
Flag	Flag of the (S, G) entry or the outgoing interface in the entry. This field displays one flag or the sum of multiple flags. In this example, the value 0x2 means that the entry has only one flag 0x2. The value 0x14 means that the interface has flags 0x4 and 0x10. The following flags are available for an entry: • **0x1**—The entry is created because of packets passed through between cards. • **0x2**—The entry is added by IPv6 multicast forwarding. The following flags are available for an outgoing interface: • **0x1**—The interface is added to the entry because of packets passed through between cards.

Field	Description
	• **0x2**—The interface is added to an existing entry. • **0x4**—The MAC address of the interface is needed for fast forwarding. • **0x8**—The interface is an outgoing interface associated with the incoming VLAN or super VLAN interface. • **0x10**—The interface is associated with the entry. • **0x20**—The interface is to be deleted.
Status	Status of the (S, G) entry or the outgoing interface: • **Enabled**—Available. • **Disabled**—Unavailable.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces	Outgoing interface list of the (S, G) entry.

New command: reset ipv6 multicast fast-forwarding cache

Use **reset ipv6 multicast fast-forwarding cache** to clear IPv6 multicast fast forwarding entries.

Syntax

Centralized devices:

reset ipv6 multicast [vpn-instance *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** }

Distributed devices in standalone mode:Centralized IRF devices:

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**slot** *slot-number*]

Distributed devices in IRF mode:

reset ipv6 multicast [**vpn-instance** *vpn-instance-name*] **fast-forwarding cache** { { *ipv6-source-address* | *ipv6-group-address* } * | **all** } [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, this command clears IPv6 multicast fast forwarding entries on the public network.

ipv6-source-address: Specifies an IPv6 multicast source address.

ipv6-group-address: Specifies an IPv6 multicast group address. The value range for this argument is FFxy::/16 (excluding FFx1::/16 and FFx2::/16), where "x" and "y" represent any hexadecimal numbers from 0 to F.

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears IPv6 multicast fast forwarding entries for the MPU. (Distributed devices in standalone mode.)

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears IPv6 multicast fast forwarding entries for the master device. (Centralized IRF devices.)

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. If you do not specify a card, this command clears IPv6 multicast fast forwarding entries for the global active MPU. (Distributed devices in IRF mode.)

Examples

# Clear all IPv6 multicast fast forwarding entries on the public network

```
<Sysname> reset ipv6 multicast fast-forwarding cache all
```

# Clear the IPv6 multicast fast forwarding entry for IPv6 multicast source and group (FE1F:20::2, FF0E::1) on the public network.

```
<Sysname> reset ipv6 multicast fast-forwarding cache fe1f:20::2 ff0e::1
```

New feature: Attack defense policy application to a security zone

Applying an attack defense policy to a security zone

To apply an attack defense policy to a security zone:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter security zone view.	**security-zone name** *Trust*	N/A
3. Apply an attack defense policy to the security zone.	**attack-defense apply policy** *policy-number*	By default, a security zone has no attack defense policy applied.

Command reference

The following commands were newly added:

- **attack-defense apply policy**
- **blacklist enable**
- **client-verify dns enable**
- **client-verify http enable**
- **client-verify tcp enable**
- **display attack-defense flood statistics ip**
- **display attack-defense flood statistics ipv6**
- **display attack-defense scan attacker ip**
- **display attack-defense scan attacker ipv6**
- **display attack-defense scan attacker ipv6**
- **display attack-defense scan victim ipv6**
- **display attack-defense statistics security-zone**
- **reset attack-defense statistics security-zone**

For information about the commands, see attack defense commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: AAA support for IKE extended authentication

Configuring IKE extended authentication

For information about this feature, see AAA configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **authentication ike** command was newly added.

The **ike** keyword was added to the **display local-user**, **undo local-user**, **service-type**, and **undo service-type** commands.

For information about the commands, see AAA commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Percentage-based CAR

Configuring percentage-based CAR

For information about this feature, see QoS in *H3C MSR Router Series Comware 7 ACL and QoS Configuration Guide*.

Command reference

The **percent car** command was added.

For information about the command, see traffic behavior commands in *H3C MSR Router Series Comware 7 ACL and QoS Command Reference*.

New feature: Logging OSPF router ID conflict events

Logging OSPF router ID conflict events

For information about this feature, see OSPF configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide*.

Command reference

The following commands were newly added:

- **database-filter peer** (OSPF view)
- **ospf database-filter**
- **ospf ttl-security**
- **ttl-security**

For information about the commands, see OSPF commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: AFT

Configuring AFT

For information about this feature, see AFT in *H3C MSR Router Series Comware 7 Layer 3—IP Services Configuration Guide*.

Command reference

For information about the commands, see AFT commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Configuring enhanced CC authentication in FIPS mode

Configuring enhanced CC authentication in FIPS mode

For information about this feature, see IPsec, SSH, SSL, and public key management in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **ecdsa** keyword was added to the following commands:

- **scp**.
- **scp ipv6**.
- **sftp**.
- **sftp ipv6**.
- **ssh2**.
- **ssh2 ipv6**.

The **dhe_rsa_aes_128_cbc_sha** and **dhe_rsa_aes_256_cbc_sha** keywords were removed from the **ciphersuite** command in FIPS mode.

The **secp192r1** and **secp256r1** keywords were added to the **public-key local create** command.

The **public-key local export ecdsa** command was added.

For more information about these commands, see IPsec, SSH, SSL, and public key management commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Support of AAA for NETCONF

Configuring support of AAA for NETCONF

For information about this feature, see AAA in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **radius session-control client** command was newly added. The **security-policy-server** command was deleted.

For information about the command, see AAA commands in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

New feature: Mobile IP tunnel interface settings

Configuring the mobile IP tunnel interface settings

Step	Command	Remarks
4. Enter system view.	**system-view**	N/A
5. Enable the mobile router feature and enter mobile router view.	**ip mobile router**	By default, the mobile router feature is disabled.

Step	Command	Remarks
6. Assign a home address to the mobile router.	**address** *ip-address*	By default, the mobile router does not have any home addresses.
7. Specify the IP address of the home agent for the mobile router.	**home-agent** *ip-address*	By default, no home agent is specified for the mobile router.
8. (Optional.) Set the MTU for the mobile IP tunnel interface.	**tunnel mtu** *value*	By default, the MTU for the tunnel interface is 64000 bytes.
9. (Optional.) Set the DF bit to 0 for outgoing tunneled packets.	**ip df-bit zero**	By default, the DF bit of outgoing tunneled packets is not set.
10. (Optional.) Apply an IPsec policy to the mobile IP tunnel interface.	**ipsec policy** *policy-name*	By default, no IPsec policy is applied to the mobile IP tunnel interface.
11. (Optional.) Set the TCP MSS for the mobile IP tunnel interface.	**tcp mss** *value*	By default, no TCP MSS is set.

Command reference

The following commands were added:

- **ip df-bit zero**
- **ipsec policy**
- **tcp mss**

For information about the commands, see NEMO commands in *H3C MSR Router Series Comware 7 NEMO Command Reference*.

New feature: LISP

Configuring LISP

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

For information about the commands, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: LISP tunnel entries and dynamic mobility

Configuring LISP tunnel entries and dynamic mobility

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

For information about the commands, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: Support of IPv6 multicast routing for VPN instances

Enabling support of IP multicast routing for VPN instances

For information about this feature, see IPv6 multicast routing and forwarding in *H3C MSR Router Series Comware 7 IP Multicast Configuration Guide.*

Command reference

The **ipv6 multicast routing vpn-instance** command was added.

For information about the command, see IPv6 multicast routing and forwarding commands in *H3C MSR Router Series Comware 7 IP Multicast Command Reference.*

New feature: LISP virtual machine multi-hop mobility and DDT

Configuring LISP virtual machine multi-hop mobility and DDT

For information about this feature, see LISP configuration in *H3C MSR Router Series Comware 7 LISP Configuration Guide*.

Command reference

The **eid-notify** command was newly added.

For information about the command, see LISP commands in *H3C MSR Router Series Comware 7 LISP Command Reference*.

New feature: LISP NSR

Configuring LISP NSR

The **display system internal lisp forwarding statistics** command was added. You can use the command to display the LISP thread statistics.

The **display system internal lisp nsr no-cache** command was added. You can use the command to display the tentative entries created during the NSR active/standby switchover.

The **display system internal lisp nsr status** command was added. You can use the command to display the LISP NSR status.

Command reference

The following commands were newly added:

- **display system internal lisp forwarding statistics**
- **display system internal lisp nsr no-cache**
- **display system internal lisp nsr status**

For information about the commands, see LISP probe commands in *H3C MSR Router Series Comware 7 Probe Command Reference*.

New feature: PPPoE client support for IPv6

Associating a dial rule with a dialup interface

For information about this feature, see DDR in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Configuration Guide*.

Command reference

The **ipv6** keyword is added to the **dialer-group rule** command. For information about this command, see DDR commands in *H3C MSR Router Series Comware 7 Layer 2—WAN Access Command Reference*.

Specifying an IPv6 prefix for an interface to automatically generate an IPv6 global unicast address

For information about this feature, see IPv6 basics in *H3C MSR Router Series Comware 7 Layer 3—IP Services Configuration Guide*.

Command reference

The **ipv6 address** command is added. For information about the command, see IPv6 basics commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: DPI engine and content filtering

Configuring the DPI engine and content filtering

For information about this feature, see DPI overview and DPI engine in *H3C MSR Router Series Comware 7 DPI Configuration Guide.*

Command reference

For information about the commands, see DPI overview and DPI engine commands in *H3C MSR Router Series Comware 7 DPI Command Reference.*

New feature: IPS

Configuring IPS

For information about this feature, see IPS configuration in *H3C MSR Router Series Comware 7 DPI Configuration Guide.*

Command reference

For information about the commands, see IPS commands in *H3C MSR Router Series Comware 7 DPI Command Reference.*

New feature: NBAR

Configuring NBAR

For information about this feature, see APR in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The following new commands were added:

- **apr signature update**.

- **Description**.
- **Destination**.
- **Direction**.
- **Disable**.
- **display app-group**.
- **display application**.
- **display apr signature information**.
- **include app-group**.
- **nbar application**.
- **nbar protocol-discovery**.
- **service-port**.
- **signature**.
- **source**.

For information about the commands, see APR in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: URL filtering

Configuring URL filtering

For information about this feature, see URL filtering configuration in *H3C MSR Router Series Comware 7 DPI Configuration Guide.*

Command reference

For information about the commands, see URL filtering commands in *H3C MSR Router Series Comware 7 DPI Command Reference.*

New feature: Local portal Web server

Configuring a local portal Web server

For information about this feature, see portal in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The following commands were added:

- **portal local-web-server**

- **default-logon-page**
- **logon-page**
- **tcp-port**

The **ssid** keyword was added to the **url-parameter** *param-name* { **apmac** | **original-url** | **source-address** | **source-mac** | **ssid** | **value** *expression* } command.

For information about the commands, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Support of portal for NETCONF

Support for NETCONF was added to portal.

New feature: Newly-added MIB objects

Event MIB added support for the hh3cWirelessCardModemMode and hh3cWirelessCardCurNetConn MIB objects.

New feature: IPS, ACG, and SSL VPN licenses

This release added support for IPS, ACG and SSL VPN licenses.

New feature: Support of NQA for NETCONF

Support for NETCONF was added to NQA.

New feature: Configuring CWMP to support VPN

Configuring CWMP to support VPN

For information about this feature, see CWMP configuration in *H3C MSR Router Series Comware 7 Network Management and Monitoring Configuration Guide*.

Command reference

For information about the commands, see CWMP commands in *H3C MSR Router Series Comware 7 Network Management and Monitoring Command Reference*.

New feature: Transceiver module source alarm

Disabling transceiver module source alarm

For information about this feature, see device management in *H3C MSR Router Series Comware 7 Fundamentals Configuration Guide*.

Command reference

transceiver phony-alarm-disable

For information about this command, see device management commands in *H3C MSR Router Series Comware 7 Fundamentals Command Reference*.

New feature: VLAN interface performance optimization

This software version optimized the following items:

- VLAN functions used for sending data in the adaption layer.
- Processing flow of the RAW functions for sending and receiving data for chips mv88ex, mvcpss, and bcm5614x.

New feature: NAT support for multicast source address in PIM join/prune packets

This feature enables the device to act as a NAT gateway and perform NAT on the multicast source address in PIM join or prune packets based on NAT mappings. Use this feature in a multicast scenario where the multicast source resides on a private network, multicast receivers reside on private networks, and PIM-SSM mode is used.

New feature: GDOI GM group anti-replay window

Configuring the anti-replay window for a GDOI GM group

Step	Command	Remarks
12. Enter system view.	**system-view**	N/A
13. Create a GDOI GM group and enter GDOI GM group view.	**gdoi gm group** [**ipv6**] *group-name*	By default, no GDOI GM groups exist.

Step	Command	Remarks
14. (Optional.) Set the anti-replay window size for the GDOI GM group.	**client anti-replay window** { **sec** *seconds* | **msec** *milliseconds* }	By default, the anti-replay window size is not set for a GDOI GM group.

Command reference

client anti-replay window

Use **client anti-replay window** to set the anti-replay window size for a GDOI GM group.

Use **undo client anti-replay window** to restore the default.

Syntax

client anti-replay window { **sec** *seconds* **|** **msec** *milliseconds* }

undo client anti-replay window

Default

The anti-replay window size is not set for a GDOI GM group.

Views

GDOI GM group view

Predefined user roles

network-admin

Parameters

sec *seconds*: Specifies the anti-replay window size in seconds in the range of 1 to 100.

msec *milliseconds*: Specifies the anti-replay window size in milliseconds in the range of 100 to 10000.

Usage guidelines

The anti-replay window size set in this command takes priority over the anti-replay window size obtained from the KS. If you do not configure this command, the anti-replay window size obtained from the KS is used.

This command must be used together with the Cisco IP-D3P feature.

Examples

# Set the anti-replay window size to 50 seconds for GDOI GM group **group1**.

```
<Sysname> system-view
[Sysname] gdoi gm group group1
[Sysname-gdoi-gm-group-group1] client anti-replay window sec 50
```

New feature: SIP compatibility

Configuring SIP compatibility

If a third-party device does not implement SIP in strict accordance with the RFC standard, you can configure SIP compatibility for the router to interoperate with the third-party device.

With the **sip-compatible t38** command configured, the router excludes **:0** from the following SDP parameters in the originated re-INVITE messages:

- T38FaxTranscodingJBIG.
- T38FaxTranscodingMMR.
- T38FaxFillBitRemoval.

With the **sip-compatible x-param** command configured, the router adds SDP description information (a=X-fax and a=X-modem) for fax pass-through and modem pass-through in the originated re-INVITE messages.

To configure SIP compatibility:

Step	Command	Remarks
15. Enter system view.	**system-view**	N/A
16. Enter voice view.	**voice-setup**	N/A
17. Enter SIP view.	**sip**	N/A
18. Configure SIP compatibility.	**sip-compatible** { **t38** | **x-param** }	By default, SIP compatibility is not configured.

Command reference

New command:sip-compatible

Use **sip-compatible** to configure SIP compatibility with a third-party device.

Use **undo sip-compatible** to restore the default.

Syntax

sip-compatible { **t38** | **x-param** }

undo sip-compatible { **t38** | **x-param** }

Default

SIP compatibility is not configured.

Views

SIP view

Predefined user roles

network-admin

Parameters

t38: Configures SIP compatibility for standard T.38 fax. With this keyword specified, the router excludes **:0** from the following SDP parameters in the originated re-INVITE messages:

- T38FaxTranscodingJBIG.
- T38FaxTranscodingMMR.
- T38FaxFillBitRemoval.

This keyword is required when the router interoperates with a third-party softswitch device to exchange T.38 fax messages.

x-param: Configures SIP compatibility for fax pass-through and modem pass-through. With this keyword specified, the router adds SDP description information for fax pass-through and modem pass-through to outgoing re-INVITE messages. This keyword is required when the router interoperates with a third-party softswitch device to perform fax pass-through and modem pass-through.

Usage guidelines

The **t38** and **x-param** keywords can be both configured to interoperate with a third-party softswitch device.

Examples

# Configure SIP compatibility for standard T.38 fax.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-compatible t38
```

New feature: Voice VLAN

Configuring a voice VLAN

Configuring a port to operate in automatic voice VLAN assignment mode

Step	Command	Remarks
19. Enter system view.	**system-view**	N/A
20. (Optional.) Set the voice VLAN aging timer.	**voice-vlan aging** *minutes*	By default, the aging timer of a voice VLAN is 1440 minutes.
21. (Optional.) Enable the voice VLAN security mode.	**voice-vlan security enable**	By default, the voice VLAN security mode is enabled.
22. (Optional.) Add an OUI address for voice packet identification.	**voice-vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	By default, system default OUI addresses exist.

Step	Command	Remarks
23. Enter interface view.	- Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* - Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* - Enter S-channel interface view: **interface s-channel** *interface-number.channel-id* - Enter S-channel aggregate interface view: **interface schannel-aggregation** *interface-number:channel-id* - Enter Layer 2 RPR logical interface view: **interface rpr-bridge** *interface-number*	N/A
24. Set the link type of the port.	- Set the port link type to trunk: **port link-type trunk** - Set the port link type to hybrid: **port link-type hybrid**	N/A
25. Configure the port to operate in automatic voice VLAN assignment mode.	**voice-vlan mode auto**	By default, the automatic voice VLAN assignment mode is enabled.
26. Enable the voice VLAN feature on the port.	**voice-vlan** *vlan-id* **enable**	By default, the voice VLAN feature is disabled on a port. Before you execute this command, make sure the specified VLAN already exists.

Configuring a port to operate in manual voice VLAN assignment mode

Step	Command	Remarks
27. Enter system view.	**system-view**	N/A
28. (Optional.) Enable the voice VLAN security mode.	**voice-vlan security enable**	By default, the voice VLAN security mode is enabled.
29. (Optional.) Add an OUI address for voice packet identification.	**voice-vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	By default, system default OUI addresses exist.

Step	Command	Remarks
30. Enter interface view.	- Enter Layer 2 Ethernet interface view: **interface** *interface-type interface-number* - Enter Layer 2 aggregate interface view: **interface bridge-aggregation** *interface-number* - Enter S-channel interface view: **interface s-channel** *interface-number.channel-id* - Enter S-channel aggregate interface view: **interface schannel-aggregation** *interface-number*:*channel-id* - Enter Layer 2 RPR logical interface view: **interface rpr-bridge** *interface-number*	N/A
31. Configure the port to operate in manual voice VLAN assignment mode.	**undo voice-vlan mode auto**	By default, a port operates in automatic voice VLAN assignment mode.
32. Set the link type of the port.	- Set the port link type to access: **port link-type access** - Set the port link type to trunk: **port link-type trunk** - Set the port link type to hybrid: **port link-type hybrid**	By default, each port is an access port.
33. Assign the access, trunk, or hybrid port to the voice VLAN.	- For the access port: **port access vlan** *vlan-id* - For the trunk port: **port trunk permit vlan** { *vlan-id-list* | **all** } - For the hybrid port: **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	After you assign an access port to the voice VLAN, the voice VLAN becomes the PVID of the port.
34. (Optional.) Configure the voice VLAN as the PVID of the trunk or hybrid port.	- For the trunk port: **port trunk pvid vlan** *vlan-id* - For the hybrid port: **port hybrid pvid vlan** *vlan-id*	This step is required for untagged incoming voice traffic and prohibited for tagged incoming voice traffic.
35. Enable the voice VLAN feature on the port.	**voice-vlan** *vlan-id* **enable**	By default, the voice VLAN feature is disabled on a port. Before you execute this command, make sure the specified VLAN already exists.

Enabling LLDP for automatic IP phone discovery

Step	Command	Remarks
36. Enter system view.	**system-view**	N/A
37. Enable LLDP for automatic IP phone discovery.	**voice-vlan track lldp**	By default, LLDP for automatic IP phone discovery is disabled.

Configuring LLDP to advertise a voice VLAN

For IP phones that support LLDP, the device advertises the voice VLAN information to the IP phones through LLDP-MED TLVs.

To configure LLDP to advertise a voice VLAN:

Step	Command	Remarks
38. Enter system view.	**system-view**	N/A
39. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
40. Configure an advertised voice VLAN ID.	**lldp tlv-enable med-tlv network-policy** *vlan-id*	By default, no advertised voice VLAN ID is configured.

Configuring CDP to advertise a voice VLAN

If an IP phone supports CDP but does not support LLDP, it sends CDP packets to the device to request the voice VLAN ID. If the IP phone does not receive the voice VLAN ID within a time period, it sends out untagged voice packets. These untagged voice packets cannot be differentiated from other types of packets.

You can configure CDP compatibility on the device to enable it to perform the following operations:

- Receive and identify CDP packets from the IP phone.
- Send CDP packets to the IP phone. The voice VLAN information is carried in the CDP packets.

After receiving the advertised VLAN information, the IP phone starts automatic voice VLAN configuration. Packets from the IP phone will be transmitted in the dedicated voice VLAN.

To configure CDP to advertise a voice VLAN:

Step	Command	Remarks
41. Enter system view.	**system-view**	N/A
42. Enable CDP compatibility.	**lldp compliance cdp**	By default, CDP compatibility is disabled.
43. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
44. Configure CDP-compatible LLDP to operate in TxRx mode.	**lldp compliance admin-status cdp txrx**	By default, CDP-compatible LLDP operates in **disable** mode.
45. Configure an advertised voice VLAN ID.	**cdp voice-vlan** *vlan-id*	By default, no advertised voice VLAN ID is configured.

Displaying and maintaining voice VLANs

Execute **display** commands in any view.

Task	Command
Display the voice VLAN state.	**display voice-vlan state**
Display OUI addresses on a device.	**display voice-vlan mac-address**

Command reference

The following commands were added:

- **display voice-vlan mac-address**.
- **display voice-vlan state**.
- **voice-vlan aging**.
- **voice-vlan enable**.
- **voice-vlan mac-address**.
- **voice-vlan mode auto**.
- **voice-vlan security enable**.
- **voice-vlan track lldp**.

For more information about these commands, see *H3C MSR Series Routers Layer 2—LAN Switching Command Reference(V7)*.

New feature: L2TP-based EAD

Enabling L2TP-based EAD

EAD authenticates PPP users that pass the access authentication. PPP users that pass EAD authentication can access network resources. PPP users that fail EAD authentication can only access the resources in the quarantine areas.

EAD uses the following procedure:

1. The iNode client uses L2TP to access the LNS. After the client passes the PPP authentication, the CAMS/IMC server assigns isolation ACLs to the LNS. The LNS uses the isolation ACLs to filter incoming packets.
2. After the IPCP negotiation, the LNS sends the IP address of the CAMS/IMC server to the iNode client. The server IP address is permitted by the isolation ACLs.
3. The CAMS/IMC sever authenticates the iNode client and performs security check for the iNode client. If the iNode client passes security check, the CAMS/IMC server assigns security ACLs for the iNode client to the LNS. The iNode client can access network resources.

To enable L2TP-based EAD:

Step	Command	Remarks
46. Enter system view.	**system-view**	N/A

Step	Command	Remarks
47. Create a VT interface and enter its view	**interface virtual-template** *virtual-template-number*	N/A
48. Enable L2TP-based EAD.	**ppp access-control enable**	By default, L2TP-based EAD is disabled.

Command reference

ppp access-control enable

Use **ppp access-control enable** to enable L2TP-based EAD.

Use **undo ppp access-control enable** to disable L2TP-based EAD.

Syntax

ppp access-control enable

undo ppp access-control enable

Default

L2TP-based EAD is disabled.

Views

VT interface view

Predefined user roles

network-admin

Usage guidelines

This command does not apply to VA interfaces that already exist in the VT interface. It only applies to newly created VA interfaces.

Different ACLs are required for different users if the VT interface is used as the access interface for the LNS.

After L2TP-based EAD is enabled, the LNS transparently passes CAMS/IMC packets to the iNode client to inform the client of EAD server information, such as the IP address.

Examples

# Enable L2TP-based EAD.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] ppp access-control enable
```

display ppp access-control interface

Use **display ppp access-control interface** to display access control information for VA interfaces on a VT interface.

Syntax

display ppp access-control interface { *interface-type interface-number* | *interface-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number.

interface-name: Specifies an interface by its name.

Examples

# Display access control information for VA interfaces on VT interface 2.

```
<Sysname> display ppp access-control interface virtual-template 2
Interface: Virtual-Template2:0
  User Name: mike
  In-bound Policy: acl 3000
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.

  Interface: Virtual-Template2:1
  User Name: tim
  In-bound Policy: acl 3001
  Totally 0 packets, 0 bytes, 0% permitted,
  Totally 0 packets, 0 bytes, 0% denied.
```

Table 3 Command output

Field	Description
Interface	VA interface that the PPP user accesses.
User Name	Username of the PPP user.
In-bound Policy	Security ACLs for the PPP user.
Totally x packets, x bytes, x% permitted	Total number, data rate, and pass percentage of permitted packets.
Totally x packets, x bytes, x% denied	Total number, data rate, and reject percentage of denied packets.

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 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 *H3C MSR Router Series Comware 7 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 source and destination IP addresses cannot be the same.
- The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode.
- As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.
- Make sure the number of member ports in a BFD-enabled aggregation group is not larger than the number of BFD sessions supported by the device. Otherwise, this command might cause some Selected ports in the aggregation group to change to the Unselected state.

Configuration procedure

To enable BFD for an aggregation group:

Step	Command	Remarks
49. Enter system view.	**system-view**	N/A
50. Enter Layer 3 aggregate interface view.	**interface route-aggregation** *interface-number*	N/A
51. 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 unicast source IP address of BFD sessions. The source IP address cannot be 0.0.0.0.

destination *ip-address*: Specifies the unicast destination IP address of BFD sessions. The destination IP address cannot be 0.0.0.0.

Usage 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 source and destination IP addresses cannot be the same.

The BFD parameters configured on an aggregate interface take effect on all BFD sessions in the aggregation group. BFD sessions for link aggregation do not support the echo packet mode and the Demand mode. For more information about BFD, see *H3C MSR Router Series Comware 7 High Availability Configuration Guide*.

As a best practice, do not configure other protocols to collaborate with BFD on a BFD-enabled aggregate interface.

Make sure the number of member ports in a BFD-enabled aggregation group is not larger than the number of BFD sessions supported by the device. Otherwise, this command might cause some Selected ports in the aggregation group to change to the Unselected state.

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: 4G modem IMSI/SN binding authentication

This feature includes the IMSI/SN information in the 4G dial-up authentication information.

Command reference

apn

Use **apn** to create an access point name (APN).

Use **undo apn** to remove an APN.

Syntax

apn { **dynamic** | **static** *apn* }

undo apn

Default

No APN is configured.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

dynamic: Uses an APN automatically assigned by the service provider.

static *apn*: Specifies the APN provided by the service provider. It is a string of 1 to 100 characters. Whether the string is case-sensitive varies by service providers.

Usage guidelines

You must specify an APN for a 4G dial-up profile.

Examples

# Specify the APN **apn1** for the 4G dial-up profile **test**.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] apn static apn1
```

apn-profile

Use **apn-profile** to create a 4G dial-up profile.

Use **undo apn-profile** to remove a 4G dial-up profile.

Syntax

apn-profile *profile-name*

undo apn-profile *profile-name*

Default

No 4G dial-up profiles are configured.

Views

System view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a 4G dial-up profile name.

Usage guidelines

A 4G dial-up profile takes effect only after you associate the profile with a 4G interface. To remove a 4G dial-up profile, you must first remove the association between the profile and the 4G interface.

Examples

# Create the 4G dial-up profile **test**.

```
<Sysname> system-view
[Sysname] apn-profile test
```

apn-profile apply

Use **apn-profile apply** to specify a 4G dial-up profile.

Use **undo apn-profile apply** to restore the default.

Syntax

apn-profile apply *profile-name* [**backup** *profile-name*]

undo apn-profile apply

Default

No 4G dial-up profiles are specified.

Views

Eth-channel interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a primary 4G dial-up profile name.

backup *profile-name*: Specifies a backup 4G dial-up profile name.

Usage guidelines

After you specify a 4G dial-up profile for a 4G modem, the 4G modem uses the settings in the profile to negotiate with the service provider's device.

The primary profile always has priority over the backup profile. For each dialup connection establishment, the 4G modem uses the backup profile only when it has failed to dial up using the primary profile.

This command takes effect only on dialup connections initiated after the command is configured. It does not take effect on a dialup connection that has been established.

Examples

# Specify the primary 4G dial-up profile **test** and the backup 4G dial-up profile **bktest** for Eth-channel interface 2/4/0:0.

```
<Sysname> system-view
[Sysname] interface eth-channel 2/4/0:0
[Sysname-Eth-channel2/4/0:0] apn-profile apply test backup bktest
```

attach-format

Use **attach-format** to set a separator for the authentication information to be sent.

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

Syntax

attach-format imsi-sn split *splitchart*

undo attach-format imsi-sn split

Default

No separator is set for the authentication information to be sent.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

split *splitchart*: Specifies a separator. It can be a letter, a digit, or a sign such as a percent sign (%) or a pound sign (#).

Usage guidelines

If IMSI/SN binding authentication is enabled, the IMSI/SN information is included in the authentication information in addition to the username. You need to configure a separator to separate different types of information. For example, if you specify the separator as #, the authentication information will be sent in the following format: *imsiinfo#sninfo#username*.

Examples

# Configure the pound sign (#) as the separator for the authentication information to be sent.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] attach-format imsi-sn split #
```

authentication-mode

Use **authentication-mode** to specify an authentication mode for a 4G dial-up profile.

Use **undo authentication-mode** to restore the default.

Syntax

authentication-mode { **pap** | **chap**| **pap-chap** } **user** *user-name* **password** { **cipher** | **simple** } *password*

undo authentication-mode

Default

No authentication mode is configured for a 4G dial-up profile.

Views

4G dial-up profile view

Predefined user roles

network-admin

Parameters

chap: Specifies CHAP authentication.

pap: Specifies PAP authentication.

pap-chap: Specifies CHAP or PAP authentication.

user *username*: Specifies the username for authentication, a case-sensitive string of 1 to 32 characters.

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

password: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 32 characters. Its encrypted form is a case-sensitive string of 1 to 73 characters

Examples

# Specify the CHAP authentication mode for the 4G dial-up profile **test**. Specify the CHAP authentication username as **user1** and the password as **123456**.

```
<Sysname> system-view
[Sysname] apn-profile test
[Sysname-apn-profile-test] authentication-mode chap user user1 password simple 123456
```

New feature: Media Stream Control (MSC) logging

This feature enables the router to generate MSC logs and send the logs to the information center.

Command reference

New command: sip log enable

Use **sip log enable** to enable Media Stream Control (MSC) logging.

Use **undo sip log enable** to disable MSC logging.

Syntax

sip log enable

undo sip log enable

Default

MSC logging is disabled.

Views

Voice view

Predefined user roles

network-admin

Usage guidelines

This command enables the router to generate MSC logs and send the logs to the information center. The information center outputs the logs to a destination according to an output rule. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

MSC logging is used for auditing purposes.

Examples

# Enable MSC logging.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip log enable
```

New feature: IMSI/SN binding authentication

This feature enables the device to include the IMSI/SN information in the LCP authentication information.

Command reference

ppp lcp imsi accept

Use **ppp lcp imsi accept** to enable the client to accept the IMSI binding authentication requests from the LNS.

Use **undo ppp lcp imsi accept** to restore the default.

Syntax

ppp lcp imsi accept

undo ppp lcp imsi accept

Default

The client declines the IMSI binding authentication requests from the LNS.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the client to accept the IMSI binding authentication requests from the LNS.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi accept
```

ppp lcp imsi request

Use **ppp lcp imsi request** to enable the LNS to initiate IMSI binding authentication requests.

Use **undo ppp lcp imsi request** to restore the default.

Syntax

ppp lcp imsi request

undo ppp lcp imsi request

Default

The LNS does not initiate IMSI binding authentication requests.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the LNS to initiate IMSI binding authentication requests.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi request
```

ppp lcp imsi string

Use **ppp lcp imsi string** *imsi-info* to configure the IMSI information on the client.

Use **undo ppp lcp imsi string** to delete the IMSI information on the client.

Syntax

ppp lcp imsi string *imsi-info*

undo ppp lcp imsi string

Default

The client automatically obtains the IMSI information from its SIM card.

Views

Interface view

Predefined user roles

network-admin

Parameters

imsi-info: Specifies the IMSI information, a case-sensitive string of 1 to 31 characters.

Examples

# Configure the IMSI information as **imsi1**.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi string imsi1
```

ppp lcp sn accept

Use **ppp lcp sn accept** to enable the client to accept the SN binding authentication requests from the LNS.

Use **undo ppp lcp sn accept** to restore the default.

Syntax

ppp lcp sn accept

undo ppp lcp sn accept

Default

The client declines the SN binding authentication requests from the LNS.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the client to accept the SN binding authentication requests from the LNS.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp sn accept
```

ppp lcp sn request

Use **ppp lcp sn request** to enable the LNS to initiate SN binding authentication requests.

Use **undo ppp lcp sn request** to restore the default.

Syntax

ppp lcp sn request

undo ppp lcp sn request

Default

The LNS does not initiate SN binding authentication requests.

Views

Interface view

Predefined user roles

network-admin

Examples

# Enable the LNS to initiate SN binding authentication requests.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp imsi request
```

ppp lcp sn string

Use **ppp lcp sn string** *sn-info* to configure the SN information on the client.

Use **undo ppp lcp sn string** to delete the SN information on the client.

Syntax

ppp lcp sn string *sn-info*

undo ppp lcp sn string

Default

The client automatically obtains the SN information from its SIM card.

Views

Interface view

Predefined user roles

network-admin

Parameters

sn-info: Specifies the SN information, a case-sensitive string of 1 to 31 characters.

Examples

# Configure the SN information as **sn1**.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp lcp sn string sn1
```

ppp user accept-format imsi-sn split

Use **ppp user accept-format imsi-sn split** *splitchart* to configure the separator for the received authentication information.

Use **undo ppp user accept-format** to restore the default.

Syntax

ppp user accept-format imsi-sn split *splitchart*

undo ppp user accept-format

Default

No separator is configured for the received authentication information.

Views

Interface view

Predefined user roles

network-admin

Parameters

splitchart: Specifies the separator. The separator contains one character, and it can be a letter, a digit, or any sign other than the at sign (@), slash (/), and backslash (\).

Usage guidelines

By default, the authentication information contains only the client username. If you include the IMSI or SN information in the authentication information, you need to configure the separator to separate different types of information.

If no IMSI/SN information is received from the peer during the authentication process, the IMSI/SN information split from the received authentication information is used.

Examples

# Configure the pound sign (#) as the separator for the authentication information.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user accept-format imsi-sn split #
```

ppp user attach-format imsi-sn split

Use **ppp user attach-format imsi-sn split** *splitchart* to configure the separator for the sent authentication information.

Use **undo ppp user attach-format** to restore the default.

Syntax

ppp user attach-format imsi-sn split *splitchart*

undo ppp user attach-format

Default

No separator is configured for the sent authentication information.

Views

Interface view

Predefined user roles

network-admin

Parameters

splitchart: Specifies the separator. The separator contains one character, and it can be a letter, a digit, or any sign other than the at sign (@), slash (/), and backslash (\).

Usage guidelines

By default, the authentication information contains only the client username. If you include the IMSI or SN information in the authentication information, you need to configure the separator to separate different types of information.

Examples

# Configure the pound sign (#) as the separator for the sent authentication information.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user attach-format imsi-sn split #
```

ppp user replace

Use **ppp user replace** to replace the client username with the IMSI or SN information for authentication.

Use **undo ppp user replace** to restore the default.

Syntax

ppp user replace { imsi | sn }

undo ppp user replace

Default

The client username is used for authentication.

Views

Interface view

Predefined user roles

network-admin

Examples

# Replace the client username with the IMSI information for authentication.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp user replace imsi
```

New feature: Specifying a band for a 4G modem

You can specify a band for a 4G modem.

Command reference

lte band

Use **ite band** to specify a band for a 4G modem.

Use **undo lte band** to restore the default.

Syntax

lte band *band-number*

undo lte band

Default

The default setting varies by 4G modem model.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

band-number: Specifies a band for a 4G modem. The available bands vary by modem model.

Usage guidelines

This command is supported only on the following 4G modems:

- Sierra MC7354 and MC7304.
- Long Sung U8300C, U8300W, and U8300.
- WNC DM11-2.

Examples

# Specify band 3 for Cellular 1/0.

```
<Sysname> system-view
[Sysname] controller cellular 1/0
[Sysname-Controller-Cellular1/0]lte band 3
```

New feature: Using tunnel interfaces as OpenFlow ports

The MSR 2600 routers support using tunnel interfaces as OpenFlow ports.

New feature: NETCONF support for ACL filtering

Support of NETCONF for ACL filtering was added.

Command reference

netconf soap http acl

Use **netconf soap http acl** to apply an ACL to NETCONF over SOAP over HTTP traffic.

Use **undo netconf soap http acl** to restore the default.

Syntax

netconf soap http acl { *acl-number* **|** **name** *acl-name* }

undo netconf soap http acl

Default

No ACL is applied to NETCONF over SOAP over HTTP traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**. The specified ACL must be an existing IPv4 basic ACL.

Usage guidelines

This command is not available in FIPS mode.

Only NETCONF clients permitted by the ACL can access the device through SOAP over HTTP.

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

Examples

# Use ACL 2001 to allow only NETCONF clients in subnet 10.10.0.0/16 to access the device through SOAP over HTTP.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

netconf soap https acl

Use **netconf soap https acl** to apply an ACL to NETCONF over SOAP over HTTPS traffic.

Use **undo netconf soap https acl** to restore the default.

Syntax

netconf soap https acl { *acl-number* **| name** *acl-name* }

undo netconf soap https acl

Default

No ACL is applied to NETCONF over SOAP over HTTPS traffic.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number in the range of 2000 to 2999.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. To avoid confusion, it cannot be **all**. The specified ACL must be an existing IPv4 basic ACL.

Usage guidelines

Only NETCONF clients permitted by the ACL can access the device through SOAP over HTTPS.

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

Examples

# Use ACL 2001 to allow only NETCONF clients in subnet 10.10.0.0/16 to access the device through SOAP over HTTPS.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap https acl 2001
```

New feature: WAAS

Configuring WAAS

This release added support for the Wide Area Application Services (WAAS) feature in the DATA image on the following router series:

- MSR 800.
- MSR 2600.
- MSR 3600.
- MSR 5600.

Command reference

All commands were newly added.

For more information about the commands, see WAAS commands in *H3C MSR Router Series Comware 7 Layer 3—IP Services Command Reference*.

New feature: Support for the MKI field in SRTP or SRTCP packets

This feature enables the router to add the MKI field to outgoing SRTP or SRTCP packets. You can set the length of the MKI field.

Command reference

New command: mki

Use **mki** to add the MKI field to outgoing SRTP or SRTCP packets and set the length of the MKI field.

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

Syntax

mki *mki-length*

undo mki

Default

Outgoing SRTP or SRTCP packets do not carry the MKI field.

Views

SIP view

Predefined user roles

network-admin

Parameters

mki-length: Specifies the length of the MKI field, in the range of 1 to 128 bytes.

Usage guidelines

This command takes effect only when SRTP is the media stream protocol for SIP calls. To specify SRTP as the medial stream protocol for SIP calls, use the **srtp** command.

Examples

# Add the MKI field to outgoing SRTP or SRTCP packets and set the length of the MKI field to 1 bit.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] mki 1
```

New feature: SIP domain name

This feature enables the router to populate the CONTACT header field of outgoing SIP packets with the router's SIP domain name.

Command reference

New command: sip-domain

Use **sip-domain** to populate the CONTACT header field of outgoing SIP packets with the router's SIP domain name.

Use **undo sip-domain** to restore the default.

Syntax

sip-domain *domain-name*

undo sip-domain

Default

The router populates the CONTACT header field of an outgoing SIP packet with the IP address of the outgoing interface.

Views

SIP view

Predefined user roles

network-admin

Parameters

domain-name: Specifies the SIP domain name, a case-insensitive string of 1 to 31 characters. Valid characters are letters, digits, underscore (_), hyphen (-), and dot (.).

Examples

# Populate the CONTACT header field of outgoing SIP packets with the SIP domain name **abc.com**.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-domain abc.com
```

New feature: Setting the maximum size of advertisement files

You can set the maximum size of advertisement files sent to wireless clients to 10 MB when the clients access the wireless network.

New feature: Support of VCF for NETCONF

Support for NETCONF was added to VCF.

New feature: Support of SNMP for NETCONF

Support for NETCONF was added to SNMP.

New feature: Support of file system for NETCONF

Support for NETCONF was added to file system.

New feature: Support of PoE for NETCONF

Support for NETCONF was added to PoE.

New feature: Support of RMON for NETCONF

Support for NETCONF was added to RMON.

New feature: Support of policy-based routing for NETCONF

Support for NETCONF was added to policy-based routing.

New feature: Support of BGP for NETCONF

Support for NETCONF was added to BGP.

New feature: Support of OSPF for NETCONF

Support for NETCONF was added to OSPF.

New feature: Support of ping for NETCONF

Support for NETCONF was added to ping.

New feature: Support of tracert for NETCONF

Support for NETCONF was added to tracert.

New feature: Support of L2VPN for NETCONF

Support for NETCONF was added to L2VPN.

New feature: SIP support for VRF

Configuring SIP support for VRF

For information about this feature, see SIP configuration in *H3C MSR Router Series Comware 7 Voice Configuration Guide.*

Command reference

The **vpn-instance** command was added.

For information about the command, see SIP commands in *H3C MSR Router Series Comware 7 Voice Command Reference.*

New feature: IKEv2

Configuring IKEv2

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

For information about the commands, see IPsec commands in *H3C MSR Router Series Comware 7 Command Reference*.

New feature: Specifying an IKEv2 profile for an IPsec policy

Specifying an IKEv2 profile for an IPsec policy

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **ikev2-profile** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: Bidirectional BFD control detection for RIP

Configuring bidirectional BFD control detection for RIP

For information about this feature, see RIP configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide.*

Command reference

The **bfd all-interfaces enable**, **rip bfd**, and **rip primary-path-detect bfd** commands were newly added.

For information about the commands, see RIP commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference.*

New feature: OSPF router ID autoconfiguration

Automatically obtaining an OSPF router ID

For information about this feature, see OSPF configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide.*

Command reference

The **display system internal ospf event-log router-id** command was newly added and the **auto-select** keyword was added to the **ospf** command.

For information about the commands, see OSPF commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference* and OSPF probe commands in *H3C MSR Router Series Comware 7 Probe Command Reference*.

New feature: Associating a static route with a track entry

Associating a static route with a track entry

For information about this feature, see static routing configuration in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Configuration Guide.*

Command reference

The **track** keyword was added to the **ip route-static** command.

For information about the command, see static routing commands in *H3C MSR Router Series Comware 7 Layer 3—IP Routing Command Reference*.

New feature: VLAN tag processing rule for incoming traffic

Configuring the VLAN tag processing rule for incoming traffic

For information about this feature, see *H3C MSR Router Series Comware 7 VXLAN Configuration Guide*.

Command reference

The **l2vpn rewrite inbound tag** command was added. For information about this command, see *H3C MSR Router Series Comware 7 VXLAN Command Reference*.

New feature: IP-based portal-free rule

Configuring an IP-based portal free-rule

For information about this feature, see portal authentication configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The portal free-rule command was added.

For information about the command, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Portal redirect packet statistics

Displaying/maintaining portal redirect packet statistics

For information about this feature, see portal authentication configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **display portal redirect statistics** and **reset portal redirect statistics** commands were added.

For information about the commands, see portal commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: GDVPN

Configuring GDVPN

For information about this feature, see group domain VPN configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

For information about the commands, see group domain VPN commands in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

New feature: OpenFlow instance

Configuring the OpenFlow instance mode

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **port** keyword was added to the **classification** command.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

Binding an OpenFlow instance to ports

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **port** command was added.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

Binding an port to an OpenFlow instance

For information about this feature, see OpenFlow in *H3C MSR Router Series Comware 7 OpenFlow Configuration Guide*.

Command reference

The **openflow-instance** command was added.

For information about the command, see OpenFlow commands in *H3C MSR Router Series Comware 7 OpenFlow Command Reference*.

New feature: Enabling the Extended Sequence Number (ESN) feature for an IPsec transform set

Enabling ESN for an IPsec transform set

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command reference

The **esn enable** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

New feature: Enabling Traffic Flow Confidentiality (TFC) padding for an IPsec policy

Enabling TFC padding for an IPsec policy

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command reference

The **tfc enable** command was added.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference*.

New feature: SIP session refresh

Enabling SIP session refresh

In this release, you can enable SIP session refresh for a VoIP voice entity.

Command reference

New command: voice-class sip session refresh

Use **voice-class sip session refresh** to enable SIP session refresh for a VoIP entity.

Use **undo voice-class sip session refresh** to disable SIP session refresh for a VoIP entity.

Syntax

voice-class sip session refresh [**global**]

undo voice-class sip session refresh

Default

A VoIP entity uses the global configuration for SIP session refresh.

Views

VoIP entity view

Predefined user roles

network-admin

Parameters

global: Applies the global configuration for SIP session refresh to the VoIP entity.

Usage guidelines

The configuration for SIP session refresh in VoIP entity view takes priority over that in SIP view.

Examples

# Enable SIP session refresh for VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip session refresh
```

# Apply the global configuration for SIP session refresh to VoIP entity 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 1 voip
[Sysname-voice-dial-entity1] voice-class sip session refresh global
```

Modified feature: User profile

Feature change description

This release added support for QoS policy configuration in user profile view.

Modified feature: Tunnel interface support for IPsec and VXLAN tunnel modes

1. Feature change description

This release added support for the IPsec tunnel mode and VXLAN tunnel mode on a tunnel interface.

2. Command changes

1. Modified command: interface tunnel

Old syntax

interface tunnel *number* [**mode** { **advpn** { **gre** | **udp** } [**ipv6**] | **ds-lite-aftr** | **evi** | **gre** [**ipv6**] | **ipv4-ipv4** | **ipv6** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **mpls-te** | **nve** }]

New syntax

interface tunnel *number* [**mode** { **advpn** { **gre** | **udp** } [**ipv6**] | **ds-lite-aftr** | **evi** | **gre** [**ipv6**] | **ipsec** [**ipv6**] | **ipv4-ipv4** | **ipv6** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **mpls-te** | **nve** |**vxlan** }]

Views

System view

Change description

The following parameters were added to the command:

- **mode ipsec**: Specifies the IPv4 IPsec tunnel mode.
- **mode ipsec ipv6**: Specifies the IPv6 IPsec tunnel mode.
- **mode vxlan**: Specifies the VXLAN tunnel mode.

Modified feature: PKI certificate auto-renewal

Feature change description

Support for certificate auto-renewal was added to PKI.

Command changes

Modified command: certificate request mode

Old syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

New syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string* | **renew-before-expire** *days* [**reuse-public-key**] [**auto-append common-name**]] * | **manual** }

Views

PKI domain view

Change description

The following keywords were added to the command:

- **renew-before-expire** *days*: Configures the system to automatically request a new certificate the specified number of days before the current certificate expires. The value range for the *days* argument is 0 to 365. Value 0 indicates that the request for a new certificate is made when the old certificate expires, which might cause service interruptions.
- **reuse-public-key**: Reuses the key pair in the old certificate for the new certificate. If you do not specify this keyword, the system generates a new key pair for the new certificate. The old key pair is replaced with the new one when the new certificate is received from the CA.
- **auto-append common-name**: Automatically appends random data to the common name of the PKI entity for the new certificate. If you do not specify this keyword, the common name of the PKI entity will be unchanged in the new certificate.

New command: display pki certificate renew-status

Use **display pki certificate renew-status** to display the certificate renewal status for a PKI domain.

Syntax

display pki certificate renew-status [**domain** *domain-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain-name: Specifies a PKI domain by its name, a case-insensitive string of 1 to 31 characters. The domain name cannot contain the special characters listed in **Error! Reference source not found.**. If you do not specify a domain name, this command displays the certificate renewal status for all PKI domains.

Special characters

Character name	Symbol	Character name	Symbol
Tilde	~	Dot	.
Asterisk	*	Left angle bracket	<
Backslash	\	Right angle bracket	>
Vertical bar	|	Quotation marks	"
Colon	:	Apostrophe	'

Examples

# Display the certificate renewal status for all PKI domains.

```
<Sysname> display pki certificate renew-status
Domain name: domain1
Renew time:  03:12:05 2015/12/07
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2015/05/12
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

The command output indicates that the **reuse-public-key** keyword was not configured for PKI domain **domain1** and a new key pair was created for the new certificate.

# Display the certificate renewal status for PKI domain **domain1**.

```
<Sysname> display pki certificate renew-status domain1
Domain name: domain1
Renew time:  03:12:05 2013/12/07
Renew public key:
  Key type: RSA
  Time when  key pair created: 15:40:48 2013/05/12
```

```
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
  667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
  C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
  FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
  2DA4C04EF5AE0835090203010001
```

Command output

Field	Description
Renew time	Time when a new certificate will be requested.
Renew public key	Information about the new key pair created for the certificate.
Key type	Key pair type, which can be RSA, DSA, or ECDSA.
Time when key pair created	Time when the key pair was created.
Key code	Public key data.

Modified feature: Configuring the PKI entity DN

Feature change description

Support for the **subject-dn** command was added to PKI. You can use the command to configure the full subject DN string. Each attribute can be specified multiple times with different values.

Command changes

New command: subject-dn

Use **subject-dn** to configure the DN for a PKI entity.

Use **undo subject-dn** to restore the default.

Syntax

subject-dn *dn-string*

undo subject-dn

Default

No DN is configured for a PKI entity.

Views

PKI entity view

Default command level

network-admin

Parameters

dn-string: Specifies the DN for the PKI entity, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The subject DN string is a sequence of *attribute*=*value* pairs separated by commas. Each attribute can be specified multiple times with different values. Supported DN attributes are:

- **CN**—Common-name.
- **C**—Country code.
- **L**—Locality.
- **O**—Organization.
- **OU**—Organization unit.
- **ST**—State or province.

After this command is configured, the following commands do not take effect:

- **common-name**
- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

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

Examples

# Configure the DN for PKI entity **en**.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] subject-dn
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

Modified feature: ADVPN

Feature change description

In this release, you can configure ADVPN group names and ADVPN group-to-QoS policy mappings.

Command changes

New command: advpn group

Use **advpn group** to configure an ADVPN group name.

Use **undo advpn group** to restore the default.

Syntax

advpn group *group-name*

undo advpn group

Default

No ADVPN group name is configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

Usage guidelines

This command must be configured on the tunnel interface of a spoke. The spoke sends the ADVPN group name in a hub-spoke tunnel establishment request to a hub. The hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel. If no match is found, the hub does not apply a QoS policy to the hub-spoke tunnel.

If you modify the ADVPN group name after the tunnel is established, the spoke will inform the hub of the modification. The hub will look for an ADVPN group-to-QoS policy mapping that matches the new ADVPN group name and apply the QoS policy in the new mapping.

As a best practice, do not configure an ADVPN group name and apply a QoS policy on the same tunnel interface.

Examples

# Configure **aaa** as the ADVPN group name.

```
<Sysname> system-view
[Sysname] interface tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn group aaa
```

2. New command: advpn map group

Use **advpn map group** to configure a mapping between an ADVPN group and a QoS policy.

Use **undo advpn map group** to delete a mapping between an ADVPN group and a QoS policy.

Syntax

advpn map group *group-name* **qos-policy** *policy-name* **outbound**

undo advpn map group *group-name*

Default

No ADVPN group-to-QoS policy mappings are configured.

Views

Tunnel interface view

Predefined user roles

network-admin

Parameters

group-name: Specifies the ADVPN group name. The group name is a case-insensitive string of 1 to 63 characters that can include only letters, digits, and dots (.).

qos-policy *policy-name*: Specifies the QoS policy name, a case-sensitive string of 1 to 31 characters.

outbound: Applies the QoS policy to the outbound direction.

Usage guidelines

This command must be configured on the tunnel interface of a hub. After receiving a hub-spoke tunnel establishment request from a spoke, the hub looks for an ADVPN group-to-QoS policy mapping that matches the ADVPN group name carried in the request. If a matching mapping is found, the hub applies the QoS policy in the mapping to the hub-spoke tunnel.

You can configure multiple ADVPN group-to-QoS policy mappings on a tunnel interface.

You can map multiple ADVPN groups to a QoS policy. You can map an ADVPN group to only one QoS policy.

As a best practice, do not configure an ADVPN group-to-QoS policy mapping and apply a QoS policy on the same tunnel interface.

Examples

# Configure a mapping between ADVPN group **aaa** and QoS policy **bbb** on **Tunnel1**.

```
<Sysname> system-view
[Sysname] interface Tunnel1 mode advpn gre
[Sysname-Tunnel1] advpn map group aaa qos-policy bbb outbound
```

Modified feature: Telnet redirect

Feature change description

In this release, a Telnet redirect user is authenticated by using the authentication settings for the TTY line. The device displays only Telnet redirect authentication information and the authentication result. It does not display the copyright statement.

Support for Telnet redirect authentication was removed from MSR56 routers.

Modified feature: DHCP snooping performance optimization

Feature change description

On a Layer 3 physical interface without subinterface, link aggregation, or snooping configured, the **dhcp snooping enable** command was optimized to cause only a slight impact on receiving non-DHCP packets. If you configure other services on the interface, the performance varies with the services you configure.

Modified feature: OSPF performance optimization

Feature change description

You can set a fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

The value range for the LSU packet sending interval was changed to 0 to 1000 milliseconds.

Command changes

Modified command: spf-schedule-interval

Old syntax

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

New syntax

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

Views

OSPF view

Change description

The *millisecond interval* argument was added to the command. You can specify this argument to set a fixed OSPF SPF calculation interval in the range of 0 to 10000 milliseconds.

Modified command: transmit-pacing

Syntax

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

Views

OSPF view

Change description

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

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

Modified feature: IP performance optimization

Feature change description

The device supports recording MAC addresses in TCP packets. You can also configure the device to record the MAC address of the local device in TCP packets.

Command changes

New command: tcp mac-record enable

Use **tcp mac-record enable** to enable MAC address recording in TCP packets.

Use **undo tcp mac-record enable** to disable MAC address recording in TCP packets.

Syntax

tcp mac-record enable

undo tcp mac-record enable

Default

MAC address recording in TCP packets is disabled.

Views

Interface view

Default command level

network-admin

Usage guidelines

This feature records the MAC address of the packet originator in a TCP option. When an attack occurs, the administrator can quickly locate the attack source according to the recorded MAC addresses.

Examples

# Enable MAC address recording in TCP packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 0/1
[Sysname-GigabitEthernet0/1] tcp mac-record enable
```

New command: tcp mac-record local

Use **tcp mac-record local** to record the MAC address of the local device in TCP packets.

Use **undo tcp mac-record local** to restore the default.

Syntax

tcp mac-record local *mac-address*

undo tcp mac-record local

Default

The destination MAC address is recorded.

Views

System view

Default command level

network-admin

Parameters

mac-address: Specifies the MAC address of the local device. The MAC address cannot be all 0s, broadcast MAC address, or multicast MAC address.

Usage guidelines

To make this command take effect, you must enable MAC address recording in TCP packets by using the **tcp mac-record enable** command.

Examples

# Record the MAC address of the local device 0605-0403-0201 in TCP packets.

```
<Sysname> system-view
[Sysname] tcp mac-record local 0605-0403-0201
```

Modified feature: AAA

Feature change description

Starting from this software version, you can configure the authorization method for IKE extended authentication.

Command changes

New command: authorization ike

Use **authorization ike** to configure the authorization method for IKE extended authentication.

Use **undo authorization ike** to restore the default.

Syntax

In non-FIPS mode:

authorization ike { **local** [**none**] **| none | radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization ike

In FIPS mode:

authorization ike { **local | radius-scheme** *radius-scheme-name* [**local**] }

undo authorization ike

Default

The default authorization method for the ISP domain is used for IKE extended authentication.

Views

ISP domain view

Predefined user roles

network-admin

Parameters

local: Performs local authorization.

none: Does not perform authorization.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a case-insensitive string of 1 to 32 characters.

Examples

# In ISP domain **test**, perform local authorization for IKE extended authentication.

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

```
[Sysname] domain test
[Sysname-isp-test] authorization ike local
```

# In ISP domain **test**, use RADIUS scheme **rd** as the primary authorization method and local authorization as the backup authorization method for IKE extended authentication.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ike radius-scheme rd local
```

Modified feature: Configuring a cellular interface for a 3G/4G modem

Feature change description

In this release, you can set the RSSI thresholds for a 3G/4G modem.

Command changes

New command: rssi

Use **rssi** to set the RSSI thresholds for a 3G/4G modem.

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

Syntax

rssi { **1xrtt** | **evdo** | **gsm** | **lte** } { **low** *lowthreshold* | **medium** *mediumthreshold* } *****

undo rssi { **1xrtt** | **evdo** | **gsm** | **lte** } [**low** | **medium**]

Default

The lower and upper thresholds for a 3G/4G modem are –150 dBm and 0 dBm, respectively.

Views

Cellular interface view

Predefined user roles

network-admin

Parameters

1xrtt: Specifies the 1xRTT mode.

evdo: Specifies the EVDO mode.

gsm: Specifies the GSM mode.

lte: Specifies the LTE mode.

low *lowthreshold*: Specifies the lower RSSI threshold value in the range of 0 to 150, which represent a lower RSSI threshold in the range of –150 dBm to 0 dBm. The value of *lowthreshold* cannot be smaller than the value of *mediumthreshold* because the system automatically adds a negative sign to the RSSI thresholds.

medium *mediumthreshold*: Specifies the upper RSSI threshold value in the range of 0 to 150, which represent an upper RSSI threshold in the range of –150 dBm to 0 dBm.

Usage guidelines

The device performs the following operations based on the actual RSSI of the 3G/4G modem:

- Sends a trap that indicates high RSSI when the RSSI exceeds the upper threshold.
- Sends a trap that indicates normal RSSI when the RSSI is between the lower threshold and upper threshold (included).
- Sends a trap that indicates low RSSI when the RSSI drops to or below the lower threshold.
- Sends a trap that indicates low RSSI every 10 minutes when the RSSI remains equal to or smaller than the lower threshold.

To view the RSSI change information for a 3G/4G modem, use the **display cellular** command.

Examples

# Set the lower threshold for a 3G/4G modem in GSM mode to –110 dBm.

```
<Sysname> system-view
[Sysname] interface cellular 0/0
[Sysname-Cellular0/0] rssi gsm low 110
```

Modified feature: QoS on VXLAN tunnel interfaces

Feature change description

This software version added support for QoS in the outbound direction of VXLAN tunnel interfaces.

Command changes

None.

Modified feature: Option 60 encapsulation in DHCP replies

Feature change description

Disabling Option 60 encapsulation in DHCP replies.

Modified feature: MPLS QoS support for matching the EXP field

Feature change description

In this release, MPLS QoS supports matching the EXP fields in both the topmost (first) MPLS label and the second MPLS label.

Command changes

New command: 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
```

Modified feature: MPLS QoS support for marking the EXP field

Feature change description

In this release, MPLS QoS supports marking the EXP fields in both the topmost (first) MPLS label and the second MPLS label.

Command changes

New command: 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 *second-mpls-exp-value*

undo remark second-mpls-exp *second-mpls-exp-value*

Default

No EXP value marking action for the second MPLS label is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

second-mpls-exp-value: Specifies an EXP value for the second MPLS label, in the range of 0 to 7.

Examples

# Define a traffic behavior to mark packets with EXP value 3 for the second MPLS label.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark second-mpls-exp 3
```

Modified feature: Automatic configuration

Feature change description

A limit was added to the number of automatic attempts. After the limit is reached, the automatic configuration process ends.

If you set the limit to 0, only one automatic configuration attempt is allowed.

Modified feature: User profile

Feature change description

In this release, the user profile name supports using dots (.).

Command change

Modified command: user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

Views

System view

Change description

Before modification: The user profile name is a case-sensitive string of 1 to 31 characters. Valid characters are letters, digits, and underscores (_), and the name must start with an English letter.

After modification: The user profile name is a case-sensitive string of 1 to 31 characters. Valid characters are letters, digits, underscores (_), and dots (.), and the name must start with an English letter.

Modified feature: Default size of the TCP receive and send buffer

Feature change description

The default value for the TCP receive and send buffer size was changed to 63 KB.

Command changes

Modified command: tcp window

Syntax

tcp window *window-size*

undo tcp window

Views

System view

Change description

Before modification: The default value for the *window-size* argument was 64 KB.

After modification: The default value for the *window-size* argument is 63 KB.

Modified feature: Support for per-packet load sharing

Feature change description

The **per-packet** keyword was added to the **ip load-sharing mode** command to support per-packet load sharing.

Command changes

Modified command: ip load-sharing mode

Old syntax

Centralized devices:

ip load-sharing mode per-flow [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *]

Centralized IRF devices–Distributed devices–In standalone mode:

ip load-sharing mode per-flow [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] [**slot** *slot-number*]

Distributed devices–In IRF mode:

ip load-sharing mode per-flow [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] [**chassis** *chassis-number* **slot** *slot-number*]

New syntax

Centralized devices:

ip load-sharing mode { **per-flow** [[**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] | **per-packet** }

Centralized IRF devices–Distributed devices–In standalone mode:

ip load-sharing mode { **per-flow** [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] | **per-packet** }

Distributed devices–In IRF mode:

ip load-sharing mode { **per-flow** [**dest-ip** | **dest-port** | **ip-pro** | **src-ip** | **src-port**] *] | **per-packet** }

Views

System view

Change description

The **per-packet** keyword was added to the **ip load-sharing mode** command to support per-packet load sharing.

Modified feature: Default user role

Feature change description

The default user role can be changed. The *role-name* argument was added to the **role default-role enable** command for specifying a user role as the default user role.

Command changes

Modified command: role default-role enable

Old syntax

role default-role enable

undo role default-role enable

New syntax

role default-role enable [*role-name*]

undo role default-role enable

Views

System view

Change description

Before modification: The default user role is network-operator.

After modification: The *role-name* argument was added to specify any user role that exists in the system as the default user role. The argument is a case-sensitive string of 1 to 63 characters. If you do not specify this argument, the default user role is network-operator.

Modified feature: Debugging

Feature change description

The **all** keyword and the **timeout** *time* option were removed from the **debugging** command. You can no longer use the **debugging all** command to enable debugging for all modules or specify the timeout time for the **debugging all** command.

Command changes

Modified command: debugging

Old syntax

debugging { **all** [**timeout** *time*] **|** *module-name* [*option*] }

undo debugging { **all** **|** *module-name* [*option*] }

New syntax

debugging *module-name* [*option*]

undo debugging *module-name* [*option*]

Views

User view

Change description

The following parameters were removed from the **debugging** command:

- **all**: Enables debugging for all modules.

timeout *time*: Specifies the timeout time for the **debugging all** command. The system automatically executes the **undo debugging all** command after the timeout time. The *time* argument is in the range of 1 to 1440 minutes. If you do not specify a timeout time, you must manually execute the **undo debugging all** command to disable debugging for all modules.

Modified feature: SSH username

Feature change description

In this release, an SSH username cannot be **a**, **al**, **all**, or include the following characters: \ | / : * ? < >

The at sign (@) can only be used in the username format *pureusername@domain* when the username contains an ISP domain name.

Command changes

Modified command: ssh user

Syntax

In non-FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }

undo ssh user *username*

In FIPS mode:

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | **password-publickey** **assign** { **pki-domain** *domain-name* | **publickey** *keyname* } }

undo ssh user *username*

Views

System view

Change description

Before modification: The *username* argument is a case-insensitive string of 1 to 80 characters. If the username contains an ISP domain name, use the format *pureusername@domain*.

After modification: The *username* argument is a case-insensitive string of 1 to 80 characters, excluding **a**, **al**, **all**, and the following characters: \ | / : * ? < >

The at sign (@) can only be used in the username format *pureusername@domain* when the username contains an ISP domain name. The pure username can contain 1 to 55 characters and the domain name can contain 1 to 24 characters. The whole username cannot exceed 80 characters.

Modified feature: IS-IS hello packet sending interval

Feature change description

The value range of the interval for sending hello packets was changed to 1 to 255 seconds.

Command changes

Modified command: isis timer hello

Syntax

isis timer hello *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

Views

Interface view

Change description

The value range for the *seconds* argument was changed to 1 to 255 seconds.

Modified feature: 802.1X redirect URL

Feature change description

The value range for the *url-string* argument was changed to 1 to 256 characters for the **dot1x ead-assistant url** command.

Command changes

Modified command: dot1x ead-assistant url

Syntax

dot1x ead-assistant url *url-string*

Views

System view

Change description

Before modification: The value range for the *url-string* argument is 1 to 64 characters.

After modification: The value range for the *url-string* argument is 1 to 256 characters.

Modified feature: Displaying information about NTP servers from the reference source to the primary NTP server

Feature change description

You can specify a source interface for tracing NTP servers from the reference source to the primary NTP server.

Command changes

Modified command: display ntp-service trace

Old syntax

display ntp-service trace

New syntax

display ntp-service trace [**source** *interface-type interface-number*]

Views

Any view

Change description

The **source** *interface-type interface-number* option was added to the **display ntp-service trace** command.

Modified feature: Saving, rolling back, and loading the configuration

The following configuration guidelines were added when you use NETCONF to save, roll back, or load the configuration:

- The save, rollback, and load operations supplement NETCONF requests. Performing the operations might consume a lot of system resources.

- Do not perform the save, rollback, or load operation when another user is performing the operation. If multiple users simultaneously perform the save, rollback, or load operation, the result returned to each user might be inconsistent with the user request.

Modified feature: Displaying information about SSH users

Feature change description

In this release, the **display ssh user-information** command does not display the public key name for an SSH user that uses password authentication.

Command changes

Modified command: display ssh user-information

Syntax

display ssh user-information [*username*]

Views

Any view

Change description

Before modification: The **User-public-key-name** field in the command output displays **null** for an SSH user that uses password authentication.

After modification: The **User-public-key-name** field in the command output is blank for an SSH user that uses password authentication.

Modified feature: SIP trusted nodes

Configuring SIP trusted nodes

In this release, you can enable the trusted node feature by using the **ip address trusted authenticate** command. You also can display information about SIP trusted nodes by using the **display voice ip address trusted list** command.

Command changes

The **display voice ip address trusted list** and **ip address trusted authenticate** commands were added.

New command: display voice ip address trusted list

Use **display voice ip address trusted list** to display information about trusted nodes.

Syntax

display voice ip address trusted list

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays trusted nodes in the trusted node list and call destination IP addresses.

Examples

# Display information about trusted nodes.

```
<Sysname> display voice ip address trusted list
IP address trusted authentication: Enabled

VoIP entity IP addresses:
Entity tag      State    SIP IP address
----------      -----    --------------
20              Up       192.168.4.110
53232           Down     192.168.4.210
55555           Up       192.168.4.210
9613            Up       192.168.4.125

IP address trusted list:
 192.168.4.0 255.255.255.0
 192.168.5.120 255.255.255.255
```

Command output

Field	Description
IP address trusted authentication	Whether IP address trusted authentication is enabled: • Enabled. • Disabled.
VoIP entity IP addresses	Trusted IP addresses for VoIP entities.

Field	Description
Entity tag	Tag of a VoIP entity.
State	Status of a VoIP entity: • Up. • Down.
SIP IP address	Call destination IP address of a VoIP entity.
IP address trusted list	List of trusted nodes.

New command: ip address trusted authenticate

Use **ip address trusted authenticate** to enable IP address trusted authentication.

Use **undo ip address trusted authenticate** to disable IP address trusted authentication.

Syntax

ip address trusted authenticate

undo ip address trusted authenticate

Default

IP address trusted authentication is disabled. All nodes are regarded as trusted, and the device accepts calls from any nodes.

Views

SIP view

Predefined user roles

network-admin

Usage guidelines

After you enable this feature, the device accepts calls only from trusted nodes.

For calls to be successfully established, configure the proxy server, registrars, the DNS server, and the MWI server as trusted nodes.

Examples

# Enable IP address trusted authentication.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] ip address trusted authenticate
```

Modified feature: IPsec ESP encryption algorithms

Feature change description

Support for the following IPsec ESP encryption algorithms was added in high encryption mode:

- AES algorithm in CTR mode.
- Camellia algorithm in CBC mode.
- GMAC algorithm.
- GCM algorithm.
- SM1 algorithm in CBC mode.
- SM4 algorithm.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following arguments were added to the **esp encryption-algorithm** command:

- *aes-ctr-128.*
- *aes-ctr-192.*
- *aes-ctr-256.*
- *camellia-cbc-128.*
- *camellia-cbc-192.*
- *camellia-cbc-256.*
- *gmac-128.*
- *gmac-192.*
- *gmac-256.*
- *gcm-128.*
- *gcm-192.*
- *gcm-256.*
- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*
- *sm4-cbc.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: IPsec ESP authentication algorithms

Feature change description

Support for the following IPsec ESP authentication algorithms was added:

- AES-XCBC-MAC.
- HMAC-SHA-25.
- HMAC-SHA-384.
- HMAC-SHA-512.
- HMAC-SM3.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following arguments were added to the **esp authentication-algorithm** command:

- *aes-xcbc-mac.*
- *sha256.*
- *sha384.*
- *sha512.*
- *sm3.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: IPsec AH authentication algorithms

Feature change description

Support for the following IPsec AH authentication algorithms was added:

- AES-XCBC-MAC.
- HMAC-SHA-256.
- HMAC-SHA-384.
- HMAC-SHA-512.
- HMAC-SM3.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following arguments were added to the **ah authentication-algorithm** command:

- *aes-xcbc-mac.*
- *sha256.*
- *sha384.*
- *sha512.*
- *sm3.*

For more information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Specifying an encryption algorithm for an IKE proposal

Feature change description

In this release, you can specify the following encryption algorithms for an IKE proposal:

- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The following keywords were added to the **encryption-algorithm** command:

- *sm1-cbc-128.*
- *sm1-cbc-192.*
- *sm1-cbc-256.*

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Specifying an authentication algorithm for an IKE proposal

Feature change description

In this release, you can specify the *sm3* authentication algorithm for an IKE proposal.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The *sm3* argument was added to the **authentication-algorithm** command.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Generating asymmetric key pairs

Feature change description

In this release, you can generate ECDSA key pairs by using the secp384r1 elliptic curve.

For information about this feature, see public key management in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The **secp384r1** keyword was added to the **public-key local create** command.

For information about the command, see public key management commands in *H3C MSR Router Series Comware 7 Command Reference*.

Modified feature: Specifying an ECDSA key pair for certificate request

Feature change description

In this release, you can specify an ECDSA key pair with a specific key length for certificate request. Supported key lengths are:

- 192 bits.
- 256 bits.
- 384 bits.

For information about this feature, see PKI in *H3C MSR Router Series Comware 7 Security Configuration Guide*.

Command changes

The following keywords were added to the **public-key ecdsa name** command:

- **secp192r1**.
- **secp256r1**.
- **secp384r1**.

For information about the command, see PKI commands in *H3C MSR Router Series Comware 7 Command Reference*.

Modified feature: QoS MIB

Feature change description

In this release, QoS MIB information changed.

Modified feature: Enabling PFS for an IPsec transform set

Feature change description

In this release, you can enable PFS using 256-bit or 384-bit ECP Diffie-Hellman group for an IPsec transform set.

For information about this feature, see IPsec configuration in *H3C MSR Router Series Comware 7 Security Configuration Guide.*

Command changes

The **dh-group19** and **dh-group20** keywords were added to the **pfs** command.

For information about the command, see IPsec commands in *H3C MSR Router Series Comware 7 Security Command Reference.*

Modified feature: Displaying track entry infomration

Feature change description

The following fields were added to the output of the **display track** command:

- IP route.
- VPN instance name.
- Protocol.
- Nexthop interface.

Command changes

Modified command: display track

Syntax

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

Views

Any view

Change description

The following fields were added to the command output:

- IP route.
- VPN instance name.
- Protocol.
- Nexthop interface.

Removed feature: Tiny proxy

Feature change description

The tiny proxy feature was removed.

Removed command

http-proxy

Syntax

http-proxy

undo http-proxy

Views

System view

Removed feature: Displaying switching fabric channel usage

Feature change description

Support for displaying switching fabric channel usage on interface cards was removed.

Removed command

display fabric utilization

Syntax

In standalone mode:

display fabric utilization [**slot** *slot-number*]

In IRF mode:

display fabric utilization [**chassis** *chassis-number* **slot** *slot-number*]

Views

Any view

Release 0408P05

This release has the following changes:

New feature: BGP trap support for VRF information

New feature: SSH redirect

New feature: BGP trap support for VRF information

VRF information is added to BGP traps as the context name.

New feature: SSH redirect

Configuring SSH redirect

About SSH redirect

SSH redirect provides redirect service for Stelnet clients. An Stelnet client can access a destination device by using the IP address of the SSH redirect server instead of the IP address of the destination device.

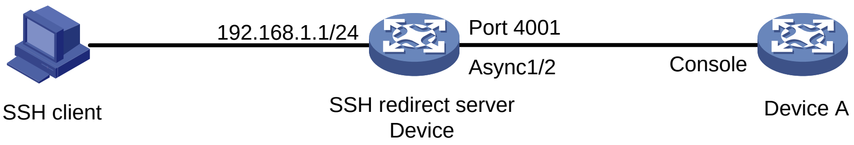
As shown in Figure 1, a user can log in to the SSH redirect server (Device) through Stelnet, and then access the destination device (Device A).

To access Device A, perform the following tasks on the PC:

1. Launch an SSH client software on the PC to establish a connection.

2. Configure connection parameters according to the authentication method.
3. Enter IP address 192.168.1.1 and listening port 4001 of the SSH redirect server.
4. When the login prompt appears on the PC, press **Enter** to enter user view of Device A.

Figure 1 Logging in to Device A through the SSH redirect server



Restrictions and guidelines

The device (SSH redirect server) allows only one login to the same destination device at a time.

Prerequisites

Before you configure SSH redirect, complete the following tasks:

- Use an asynchronous interface of the SSH redirect server to connect to the console port or AUX port of the destination device. An asynchronous interface can be a dedicated asynchronous interface or a synchronous/asynchronous serial interface operating in asynchronous mode.
- If the SSH redirect server is connected to the AUX port of the destination device, perform the following tasks:
  a. Log in to the destination device through the console port.
  b. Disable login authentication for the AUX line.

Procedure

Configuring the asynchronous serial interface

Step	Command	Remarks
52. Enter system view.	**system-view**	N/A
53. Enter synchronous/asynchronous serial interface view or asynchronous interface view.	• Enter synchronous/asynchronous serial interface view and configure it to operate in asynchronous mode: a. **interface serial** *interface-number* b. **physical-mode async** • Enter asynchronous interface view: **interface async** *interface-number*	To use a synchronous/asynchronous serial interface, you must use a connector to connect the interface to the destination device.
54. Set the operating mode to flow mode.	**async-mode flow**	By default, an asynchronous serial interface operates in

		protocol mode.
55. (Optional.) Disable level detection.	**undo detect dsr-dtr**	By default, level detection is enabled. Whether this command is required depends on the destination device.
56. Return to system view.	**quit**	N/A

Configuring the AUX/TTY user line

Step	Command	Remarks
57. Enter AUX or TTY line view.	**line** { *first-number1* [*last-number1*] | { **aux** | **tty** } *first-number2* [*last-number2*] }	N/A
58. (Optional.) Enable the terminal service.	**shell**	By default, the terminal service is enabled on all user lines.
59. Set the transmission rate.	**speed** *speed-value*	By default, the transmission rate is 9600 bps. The user line must use the same transmission rate as the destination device.
60. Enable stop bit setting consistency detection.	**stopbit-error intolerance**	By default, stop bit setting consistency detection is disabled.
61. Specify the number of stop bits.	**stopbits** { **1** | **1.5** | **2** }	By default, the number of stop bits is 1. Set the same number of stop bits for the user line on the SSH redirect server as the destination device.

Configuring SSH redirect

Step	Command	Remarks
62. Enable SSH redirect.	**ssh redirect enable**	By default, SSH redirect is disabled.
63. (Optional.) Specify an SSH redirect listening port.	**ssh redirect listen-port** *port-number*	By default, the listening port number of SSH redirect is the absolute user line number plus 4000.
64. (Optional.) Set the idle-timeout timer for the redirected connection.	**ssh redirect timeout** *time*	The default idle-timeout timer is 360 seconds.
65. (Optional.) Terminate the redirected SSH connection.	**ssh redirect disconnect**	N/A
66. Return to system view.	**quit**	N/A
67. (Optional.) Associate the SSH redirect listening port with an IP address.	**ssh ip alias** *ip-address* *port-number*	By default, an SSH redirect listening port is not associated with an IP address.

Command reference

Modified command: display ssh server

Old syntax

display ssh server { **session** | **status** }

New syntax

Centralized devices:

display ssh server { **session** | **status** }

Distributed devices in standalone mode/centralized devices in IRF mode:

display ssh server { **session** [**slot** *slot-number* [**cpu** *cpu-number*]] | **status** }

Distributed devices in IRF mode:

display ssh server { **session** [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] | **status** }

Views

Any view

Command change description

After modification, parameters were added to the command and the parameters available for a device vary by device type.

- **slot** *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays the SSH server sessions for all cards. (Distributed devices in standalone mode.)
- **slot** *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the SSH server sessions for all member devices. (Centralized IRF devices, IRF 3 incapable.)
- **slot** *slot-number*: Specifies an IRF member device by its member ID or specifies a PEX by its virtual slot number. On an IRF 2 fabric, this command displays the SSH server sessions for all member devices if you do not specify a member device. On an IRF 3 system, this command displays the SSH server sessions for all IRF 2 member devices and PEXs if you do not specify an IRF 2 member device or PEX. (Centralized IRF devices, IRF 3 capable.)
- **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. If you do not specify a card, this command displays the SSH server sessions for all cards. (Distributed devices–In IRF mode, IRF 3 incapable.)
- **chassis** *chassis-number* **slot** *slot-number*: Specifies a card on an IRF member device or specifies a PEX. The *chassis-number* argument represents the member ID of the IRF member device or the virtual chassis number of the PEX. The *slot-number* argument represents the slot

number of the card or PEX. On an IRF 2 fabric, this command displays the SSH server sessions for all member devices if you do not specify a member device. On an IRF 3 system, this command displays the SSH server sessions for all IRF 2 member devices and PEXs if you do not specify a member device or PEX. (Distributed devices–In IRF mode, IRF 3 capable.)

- **cpu** *cpu-number*: Specifies a CPU by its number. This option is available only if multiple CPUs are available on the specified slot.

New command: ssh ip alias

Use **ssh ip alias** to associate an SSH redirect listening port with an IP address.

Use **undo ssh ip alias** to delete the IP address associated with the SSH redirect listening port.

Syntax

ssh ip alias *ip-address port-number*

undo ssh ip alias *ip-address*

Default

An SSH redirect listening port is not associated with an IP address.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address to be associated with the SSH redirect listening port. The IP address cannot be the address of an interface on the device, but can be on the same subnet as the device.

port-number: Specifies an SSH redirect listening port number in the range of 4000 to 50000.

Usage guidelines

The SSH redirect server can provide the SSH redirect service after SSH redirect is enabled and an SSH redirect listening port is configured. The SSH client can use the **ssh2** *ip address port number* command to access the destination device. The *ip address* argument and the *port number* argument specify the IP address of the SSH redirect server and the SSH redirect listening port, respectively.

After the **ssh ip alias** command is configured, the client can use the **ssh2** *ip address* command to access the destination device. The *ip address* argument specifies the IP address associated with the SSH redirect listening port.

If you specify multiple SSH redirect listening ports for an IP address, the most recent configuration takes effect.

Examples

# Associate SSH redirect listening port 2000 with IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] ssh ip alias 1.1.1.1 4000
```

New command: ssh redirect disconnect

Use **ssh redirect disconnect** to terminate the redirected SSH connection.

Syntax

ssh redirect disconnect

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Examples

# Manually terminate the redirected SSH connection on TTY line 1.

```
<Sysname> system-view
[Sysname] line tty 1
[Sysname-line-tty1] ssh redirect disconnect
```

New command: ssh redirect enable

Use **ssh redirect enable** to enable SSH redirect for a user line.

Use **undo ssh redirect enable** to disable SSH redirect for a user line.

Syntax

ssh redirect enable

undo ssh redirect enable

Default

SSH redirect is disabled for a user line.

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Usage guidelines

Configure the user line connected to the destination device to use the same transmission rate and number of stop bits as the destination device. To change the transmission rate for the user line, use the **speed** command.

To identify whether the user line and the destination device are using the same number of stop bits, use the **stopbit-error intolerance** command. To change the number of stop bits, use the **stopbits** command.

For more information about the transmission rate and stop bits, see the login management configuration in *Fundamentals Configuration Guide*.

Examples

# Enable SSH redirect on TTY line 7.

```
<Sysname> system-view
[Sysname] line tty 7
[Sysname-line-tty7] ssh redirect enable
```

New command: ssh redirect listen-port

Use **ssh redirect listen-port** to set a listening port of SSH redirect.

Use **undo ssh redirect listen-port** to restore the default.

Syntax

ssh redirect listen-port *port-number*

undo ssh redirect listen-port

Default

The SSH redirect listening port number is the absolute user line number plus 4000.

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Parameters

port-number: Specifies the number of the SSH redirect listening port, in the range of 4000 to 50000.

Usage guidelines

The device redirects only SSH connection requests destined for the SSH redirect listening port.

Examples

# Set the SSH redirect listening port number to 5000 on TTY line 1.

```
<Sysname> system-view
[Sysname] line tty 1
[Sysname-line-tty1] ssh redirect listen-port 5000
```

New command: ssh redirect timeout

Use **ssh redirect timeout** to set the idle-timeout timer for the redirected SSH connection.

Use **undo ssh redirect timeout** to restore the default.

Syntax

ssh redirect timeout *time*

undo ssh redirect timeout

Default

The idle-timeout timer is 360 seconds.

Views

AUX line view

TTY line view

Predefined user roles

network-admin

Parameters

time: Specifies the idle-timeout timer in seconds. The value range is 0 to 86400. To disable the timeout mechanism, set the timeout timer to 0.

Usage guidelines

If no data is received from the SSH client before the timer expires, the user line terminates the redirected connection.

Examples

# Set the idle-timeout timer to 200 seconds for the redirected SSH connection.

```
<Sysname> system-view
[Sysname] line tty 1
[Sysname-line-tty1] ssh redirect timeout 200
```

Release 0407

None

ESS 0404P06

None

ESS 0403

None