# HP A-MSR20_A-MSR30_A-MSR50_A-MSR900-CMW520-R2209-SI Release Notes

# HP A-MSR20_A-MSR30_A-MSR50_A-MSR900-CMW520-R2209-SI Release Notes

Keywords: Version Information, Unresolved Problems and Avoidance Measure

Abstract: This release notes describes the R2209 release with respect to hardware and software compatibility, released features and functions, software upgrading, and documentation.

Acronyms:

| Acronym | Full spelling |
|---|---|
| LAN | Local Area Network |
| MAC | Media Access Control |
| IGMP | Internet Group Management Protocol |
| VLAN | Virtual Local Area Network |
| STP | Spanning Tree Protocol |
| RMON | Remote Monitor(SNMP) |
| GMRP | GARP Multicast Registration Protocol |
| ACL | Access Control List |
| DHCP | Dynamic Host Configuration Protocol |
| OSPF | Open Shortest Path First |
| RIP | Routing Information Protocol |
| ARP | Address Resolution Protocol |
| AAA | Authentication Authorization Accounting |
| RSTP | Rapid Spanning Tree Protocol |
| PIM | Protocol Independent Multicast |
| LPM | Longest Prefix Match |
| QoS | Quality of Service |
| UTP | Unshielded Twisted Paired |
| SFP | Small Form-Factor Pluggable |
| GBIC | Gigabit Interface Converter |

# Contents

# List of Tables

# Version information

## Version number

A-MSR 20-20_A-MSR 20-21_A-MSR 20-40_A-MSR30-16_A-MSR 30-20_A-MSR 30-40_A-MSR 30-60_A-MSR 50-40_A-MSR 50-60_A-MSR 50-40 MPU-G2_A-MSR 50-60 MPU-G2_A-MSR30-1X:

Comware software, Version 5.20, Release 2209, Standard

A-MSR9XX_A-MSR20-1X:

Comware software, Version 5.20, Release 2209

Note: You can see the version number with the command display version in any view. Please see Note①.

## Version history

Table 1 Version history

| Version number | Last version | Release Date | Remarks |
|---|---|---|---|
| CMW520-R2209 | CMW520-R2207P45 | 2012-02-14 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P45 | CMW520-R2207P38 | 2011-12-28 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P38 | CMW520-R2207P34 | 2011-11-18 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P34 | CMW520-R2207P23 | 2011-10-19 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P33 | CMW520-R2207P02 | 2011-10-08 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P23 | CMW520-R2207P14 | 2011-09-15 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P14 | CMW520-R2207P02 | 2011-08-17 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207P02 | CMW520-R2207 | 2011-06-23 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 series |
| CMW520-R2207 | CMW520-R2105P38 | 2011-05-19 | Support A-MSR20_30_50_900 series and MSR20_30_50_900 |

| Version number | Last version | Release Date | Remarks |
|---|---|---|---|
| | | | series |
| CMW520-R2105P38 | CMW520-R2105P36 | 2011-05-17 | Support MSR20_30_50_900 series |
| CMW520-R2105P36 | CMW520-R2105P35 | 2011-04-19 | Support MSR20_30_50_900 series |
| CMW520-R2105P35 | CMW520-R2105P31 | 2011-03-30 | Only support MSR 30_50_50 MPU-G2 series |
| CMW520-R2105P31 | CMW520-R2105P26 | 2011-03-08 | Support MSR20_30_50_900 series |
| CMW520-R2105P26 | CMW520-R2105P25 | 2011-02-16 | Support MSR20_30_50_900 series |
| CMW520-R2105P25 | CMW520-R2105P22 | 2011-01-28 | Only support MSR30-1X series |
| CMW520-R2105P22 | CMW520-R2105P12 | 2011-01-19 | Support MSR20_30_50_900 series |
| CMW520-R2105P12 | CMW520-R2105P06 | 2010-12-10 | Support MSR20_30_50_900 series |
| CMW520-R2104P09 | CMW520-R2104P02 | 2010-09-19 | Only support MSR30-1X series |
| CMW520-R2105P06 | CMW520-R2105P02 | 2010-11-25 | Support MSR20_30_50_900 series |
| CMW520-R2105P02 | CMW520-R2105 | 2010-10-15 | Support MSR20_30_50_900 series |
| CMW520-R2105 | CMW520-R2104P02 | 2010-09-13 | Support MSR20_30_50_900 series |
| CMW520-R2104P02 | First release | 2010-08-17 | Support MSR20_30_50_900 series |

# Hardware and software compatibility matrix

HP A-MSR product family matrix:

Before HP A-MSR family, there were another 2 product families, i.e. 3Com MSR and H3C MSR, shipped to market. All of these three product families have same hardware and software specification except brand. The product matrix is as following. In brief, the HP A-MSR SKU will be the representation to all of them in subsequent document.

Table 2 Product matrix

| HP A-MSR series | H3C MSR series | 3Com MSR series |
|---|---|---|
| A-MSR20-1X series: A-MSR 20-10_ A-MSR 20-11_ A-MSR 20-12_ A-MSR 20-13 (No A-MSR 20-15) | MSR20-1X series: MSR 20-10_MSR 20-11_MSR 20-12_MSR 20-13_MSR 20-15 | MSR20-1X series: MSR 20-10_MSR 20-11_MSR 20-12_MSR 20-13_MSR 20-15 |
| A-MSR 20-20_A-MSR 20-21_A-MSR 20-40 | MSR 20-20_MSR 20-21_MSR 20-40 | MSR 20-20_MSR 20-21_MSR 20-40 |
| None | MSR30-11 | None |

| HP A-MSR series | H3C MSR series | 3Com MSR series |
|---|---|---|
| A-MSR30-1X series: A-MSR30-10_A-MSR30-11E_A-MSR30-11F | Only MSR30-10 | None |
| A-MSR 30-16 | MSR 30-16 | MSR 30-16 |
| A-MSR30-20_A-MSR 30-40_A-MSR 30-60 | MSR30-20_MSR 30-40_MSR 30-60 | MSR30-20_MSR 30-40_MSR 30-60 |
| A-MSR 50-40_A-MSR 50-60_ A-MSR 50-40 MPU-G2_A-MSR 50-60 MPU-G2 | MSR 50-40_MSR 50-60_MSR 50-40 MPU-G2_MSR 50-60 MPU-G2 | MSR 50-40_MSR 50-60 |
| A-MSR9XX series: A-MSR 900_A-MSR920 | MSR9XX series: MSR 900_MSR920 | None |

Table 3 Hardware and software compatibility matrix

| Item | Specifications | | |
|---|---|---|---|
| Product family | A-MSR20_30_50_900 series routers | | |
| Hardware platform | A-MSR20-1X series: A-MSR 20-10_ A-MSR 20-11_ A-MSR 20-12_ A-MSR 20-13/MSR 20-15<br>A-MSR 20-20_A-MSR 20-21_A-MSR 20-40<br>MSR30-11<br>A-MSR30-1X series: A-MSR30-10_A-MSR30-11E_A-MSR30-11F<br>A-MSR 30-16<br>A-MSR30-20_A-MSR 30-40_A-MSR 30-60<br>A-MSR 50-40_A-MSR 50-60_ A-MSR 50-40 MPU-G2_A-MSR 50-60 MPU-G2<br>A-MSR9XX series: A-MSR 900_A-MSR920 | | |
| Boot ROM version | A-MSR20-1X series: 226 or higher<br>A-MSR 20-20_A-MSR 20-21_A-MSR 20-40: 313 or higher<br>A-MSR30-1X series: 222 or higher<br>A-MSR 30-16: 212 or higher<br>A-MSR30-20_A-MSR 30-40_A-MSR 30-60: 317 or higher<br>A-MSR 50-40_A-MSR 50-60: 315 or higher<br>A-MSR 50-40 MPU-G2_A-MSR 50-60 MPU-G2: 122 or higher<br>A-MSR9XX series: 116 or higher<br>(Note: Perform the command display version command in any view to view the version information. Please see Note②) | | |
| Host software | Hardware | software | MD5 Check Sum |
| | A-MSR 20-20_A-MSR 20-21_A-MSR 20-40 | A_MSR20-CMW520-R2209-SI.BIN | 66d81747bfe3f6a9398bcb792e7b6bdd |
| | A-MSR20-1X series | A_MSR201X-CMW520-R2209.BIN | 1cdf26d77036ec191465f796b6aa2bcb |
| | A-MSR30-1X series | A_MSR301X-CMW520-R2209-SI.BIN | d759b089088b77198a83d6b17a564481 |
| | A-MSR 30-16 | A_MSR3016-CMW520-R2 | a5a502fd7ee818554e38982c6cb |

| Item | Specifications | | |
|---|---|---|---|
| | | 209-SI.BIN | 6aaf3 |
| | A-MSR 30-20_A-MSR 30-40_A-MSR 30-60 | A_MSR30-CMW520-R2209-SI.BIN | b4bd3304a91267cd8bb5d15fe1ae59a8 |
| | A-MSR 50-40_A-MSR 50-60 | A_MSR50-CMW520-R2209-SI.BIN | 007cee3d045d9d56d52416759a8090e7 |
| | A-MSR 50-40 MPU-G2_ A-MSR 50-60 MPU-G2 | A_MSR50-CMW520-R2209-EPUSI.BIN | f995bf1df55439f06d867efbda60a078 |
| | A-MSR 900_A-MSR920 | A_MSR9XX-CMW520-R2209.BIN | 1f891222bee7e0588dd76749ac386a41 |
| iMC version | iMC PLAT 5.0 SP1 (E0101L07)<br>iMC UAM 5.0 SP1 (E0101P03)<br>iMC EAD 5.0 SP1 (E0101P03)<br>iMC MVM 5.0 (E0101L01) + H02<br>iMC VSM 5.0 (E0101H01)<br>iMC QoSM 5.0 SP1 (E0101P01) | | |
| iNode version | iNode PC 5.0 (E0103) | | |
| Cards Version | Cards Name | Software Version | CPLD or FPGA version |
| | SIC-AP | R3200 or higher | 200 or higher |
| | SIC-ADSL-I/SIC-ADSL-P | 170 or higher | 100 or higher |
| | MIM-6FCM/FIC-6FCM | 230 or higher | 100 or higher |
| | FIC-24FXS | 200 or higher | 100 or higher |
| | DFIC-24FXO24FXS | 200 or higher | 100 or higher |
| | SIC-2BSV/MIM-4BSV/FIC-4BSV | None | CPLD: 200 or higher |
| | VCPM: RTV1VCPM | None | CPLD: 100 or higher<br>FPGA: 400 or higher |

Sample: To display the host software and Boot ROM version of the A-MSR routers, perform the following:

```
<Sysname> display version
HP Comware Platform Software
Comware Software, Version 5.20, Release 2209, Standard  ------- Note①
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
HP A-MSR30-60 uptime is 0 week, 0 day, 0 hour, 1 minute
Last reboot 2011/06/02 09:58:02
System returned to ROM By <Reboot> Command.

CPU type: FREESCALE MPC8349 533MHz
512M bytes DDR SDRAM Memory
4M bytes Flash Memory
Pcb               Version:  4.0
Logic             Version:  3.0
```

```
Basic    BootROM  Version:  3.17
Extended BootROM  Version:  3.17                              ------- Note②
[SLOT  0]CON                        (Hardware)4.0    (Driver)1.0,    (Cpld)3.0
[SLOT  0]AUX                        (Hardware)4.0    (Driver)1.0,    (Cpld)3.0
[SLOT  0]GE0/0                      (Hardware)4.0    (Driver)1.0,    (Cpld)3.0
[SLOT  0]GE0/1                      (Hardware)4.0    (Driver)1.0,    (Cpld)3.0
[SLOT  0]CELLULAR0/0                (Hardware)4.0    (Driver)1.0,    (Cpld)3.0
```

# Restrictions and cautions

1. This product complies with the European Radio & Telecommunication Terminal Equipment Directive 1999/5/EC. Based on this evaluation, a minimum distance of 25 cm between the 3G antennas and between the 3G antenna and the WiFi antenna is required to maintain compliance and receiver reliability.

2. JF253B 1-Port E1/CE1/PRI SIC Module Remote Alarm Indication (RAI) handling – The module does not handle RAI correctly.

# Feature list

# Hardware features

Table 4 A-MSR20-1X Series Hardware Features

| Item | A-MSR 20-10 Description | A-MSR 20-11 Description | A-MSR 20-12 Description | A-MSR 20-13 Description | MSR 20-15 Description |
|---|---|---|---|---|---|
| Dimensions (H x W x D) | 44.2mm%300mm%240mm | 44.2mm%300mm%240mm | 44.2mm%300mm%240mm | 44.2mm%300mm%240mm | 44.2mm%300mm%240mm |
| Weight | 3Kg | 3Kg | 3Kg | 3Kg | 3Kg |
| Input AC voltage | Rated voltage: 100 VAC to 240 VAC;<br>50 Hz/60 Hz | | | | |
| Input DC voltage | Not support DC | | | | |
| Max power consumption | 25W | | | | |
| Operating temperature | 0°C to 40°C | | | | |
| Relative humidity (noncondensing) | 5% to 90% | | | | |
| Processor | PowerPC | PowerPC | PowerPC | PowerPC | PowerPC |
| BootROM | 1MB | 1MB | 1MB | 1MB | 1MB |
| FLASH | 16MB/32 MB | 16MB/32 MB | 16MB/32 MB | 16MB/32 MB | 16MB/32 MB |

| Memory | | 256MB | 256MB | 256MB | 256MB | 256MB |
|---|---|---|---|---|---|---|
| External module | SIC/ DSIC module | 1 | 1 | 1 | 1 | 1 |
| Internal module | VPM strip | 0 | 0 | 1 | 0 | 1 |
| Fixed interface | Console/AUX | 1 | 1 | 1 | 1 | 1 |
| | USB | 1 | 1 | 1 | 1 | 1 |
| | FE | 1 electrical interfaces | 1 electrical interfaces | 1 electrical interfaces | 1 electrical interfaces | 1 electrical interfaces |
| | FE switching interface | 4 | 4 | 4 | 4 | 4 |
| | ADSL | 0 | 0 | 0 | 0 | 1 |
| | G.SHDSL | 0 | 0 | 0 | 1(G.SHDSL.bis) | 0 |
| | SAE | 0 | 1 | 0 | 0 | 0 |
| | ISDN S/T | 0 | 0 | 0 | 1 | 1 |
| | AM | 0 | 0 | 0 | 0 | 1 |
| | E1/T1 | 0 | 0 | 1 | 0 | 0 |
| optional | Wlan | 1 | 0 | 1 | 1 | 1 |

Table 5 A-MSR20 Series Hardware Features

| Item | A-MSR 20-20 Description | A-MSR 20-21 Description | A-MSR 20-40 Description |
|---|---|---|---|
| Dimensions (H x W x D) | 44.2mm%360mm%287.1mm | 44.2mm%360mm%287.1mm | 44.2mm%442mm%407.1mm |
| Weight | 3.4Kg | 3.4Kg | 5.4Kg |
| Input AC voltage | Rated voltage: 100 VAC to 240 VAC; 50/60 Hz | | |
| Input DC voltage | Not support DC | | |
| Max power | 54W | 54W | 100W |
| Operating temperature | 0°C to 40°C (32oF to 104oF) | | |
| Relative humidity (noncondensing) | 5% to 90% | | |
| Processor | PowerPC | PowerPC | PowerPC |

| | | | | |
|---|---|---|---|---|
| BootROM | | 4MB | 4MB | 4MB |
| Memory | | SDRAM<br>Default: 256MB<br>Maximum: 256MB | SDRAM<br>Default: 256MB<br>Maximum: 256MB | SDRAM<br>Default: 256MB<br>Maximum: 256MB |
| CF CARD | | Default: 256MB<br>Maximum: 1GB | Default: 256MB<br>Maximum: 1GB | Default: 256MB<br>Maximum: 1GB |
| External module | SIC module | 2 | 2 | 4 |
| Internal module | ESM module | 1 | 1 | 2 |
| | VCPM module | 0 | 0 | 1 |
| | VPM strip | 0 | 0 | 2 |
| Fixed interface | Console | 1 | 1 | 1 |
| | AUX | 1 | 1 | 1 |
| | USB | 1 | 1 | 1 |
| | FE | Two electrical interfaces | Two electrical interfaces | Two electrical interfaces |
| | FE switching interface | 0 | 8 | 0 |

Table 6 A-MSR30 Series Hardware Features

| Item | MSR 30-11 Description | A-MSR 30-16 Description | A-MSR 30-20 Description | A-MSR 30-40 Description | A-MSR 30-60 Description |
|---|---|---|---|---|---|
| Dimensions (H x W x D) | 44.2mm×442 mm×360 mm | 44.2mm×442 mm×441.8mm | 44.2mm×442 mm×441.8mm | 88.2mm×442 mm×422.3mm | 132mm×442 mm×421.8mm |
| Weight | 4.6Kg | 6Kg | 6.9Kg | 11.9Kg | 13.6Kg |
| Input AC voltage | Rated voltage: 100 VAC to 240 VAC;<br>50 Hz/60 Hz | | | | |
| Input DC voltage | Not support DC | Not support DC | Rated voltage: -48V d.c.～-60V d.c | Rated voltage: -48V d.c.～-60V d.c | Rated voltage: -48V d.c.～-60V d.c |
| Max power | 54W | 100W | 125W | 210W | 210W |
| Operating temperature | 0°C to 40°C | | | | |
| Relative humidity (noncondensing) | 5% to 90% | | | | |

| Processor | | PowerPC | PowerPC | PowerPC | PowerPC | PowerPC |
|---|---|---|---|---|---|---|
| BootROM | | 2MB | 4MB | 4MB | 4MB | 4MB |
| Memory | | DDR SDRAM<br>Default: 256MB<br>Maximum: 256MB | DDR SDRAM<br>Default: 256MB<br>Maximum: 256MB | DDR SDRAM<br>Default: 512MB<br>Maximum: 1GB | DDR SDRAM<br>Default: 512MB<br>Maximum: 1GB | DDR SDRAM<br>Default: 512MB<br>Maximum: 1GB |
| CF CARD | | 0 | Default: 256MB<br>Maximum: 1GB | Default: 256MB<br>Maximum: 1GB | Default: 256MB<br>Maximum: 1GB | Default: 256MB<br>Maximum: 1GB |
| FLASH | | 32MB | 0 | 0 | 0 | 0 |
| External module | SIC module | 2 | 4 | 4 | 4 | 4 |
| | DSIC module | 0 | 2 | 2 | 2 | 2 |
| | MIM module | 1 | 1 | 2 | 4 | 6 |
| | XMIM module | 1 | 0 | 0 | 0 | 0 |
| | DMIM module | 0 | 0 | 0 | 1 | 2 |
| Internal module | ESM module | 1 | 2 | 2 | 2 | 2 |
| | VCPM module | 0 | 1 | 1 | 1 | 1 |
| | VPM strip | 0 | 2 | 2 | 3 | 3 |
| Fixed interface | Console | 1 | 1 | 1 | 1 | 1 |
| | AUX | 1 | 1 | 1 | 1 | 1 |
| | USB | 0 | 1 | 2 | 2 | 2 |
| | FE | 2 | 2 | 0 | 0 | 0 |
| | GE | 0 | 0 | 2 electrical interfaces | 2 Combo interfaces | 2 Combo interfaces |
| | SAE | 1 | 0 | 0 | 0 | 0 |

Table 7 A-MSR30 -1X Series Hardware Features

| Item | | A-MSR 30-10 Description | A-MSR 30-11E Description | A-MSR 30-11F Description |
|---|---|---|---|---|
| Dimensions (H x W x D) | | 44.2 mm×442 mm×360mm | 44.2 mm×442 mm×360mm | 44.2 mm×442 mm×360mm |
| Weight | | 4.8kg | 4.5Kg | 4.8kg |
| Input AC voltage | | Rated voltage: 100 VAC to 240 VAC; 50/60 Hz | | |
| Input DC voltage | | Rated voltage: –48 VDC to –60 VDC | Not support DC | Not support DC |
| Max power | | 54W | 54W | 54W |
| Operating temperature | | 0°C to 40°C (32oF to 104oF) | | |
| Relative humidity (noncondensing) | | 5% to 90% | | |
| Processor | | PowerPC | PowerPC | PowerPC |
| BootROM | | 2MB | 2MB | 2MB |
| Memory | | DDR SDRAM<br>Default: 256MB<br>Maximum: 256MB | DDR SDRAM<br>Default: 256MB<br>Maximum: 256MB | DDR SDRAM<br>Default: 256MB<br>Maximum: 256MB |
| CF CARD | | Not support | Not support | Not support |
| FLASH | | 256MB | 256MB | 256MB |
| External module | SIC module | 2 | 2 | 2 |
| | MIM module | 1 | 1 | 1 |
| | XMIM module | 1 | 0 | 0 |
| Internal module | ESM module | 1 | 1 | 1 |
| | VPM strip | 1 | 0 | 0 |
| Fixed interface | Console | 1 | 1 | 1 |
| | AUX | 1 | 1 | 1 |
| | USB | 1 | 1 | 1 |
| | FE | Two electrical interfaces | Two electrical interfaces | Two electrical interfaces |
| | FE switching interface | 0 | 24 | 48 |

Table 8 A-MSR50 Series Hardware Features

| Item | | A-MSR 50-40 Description | A-MSR 50-40 MPU-G2 Description | A-MSR 50-60 Description | A-MSR 50-60 MPU-G2 Description |
|---|---|---|---|---|---|
| Dimensions (H x W x D) | | 130.7mm×436.2mm×424mm | | 175.1mm×436.2mm×424mm | |
| Weight | | 18Kg | | 20Kg | |
| Input AC voltage | | Rated voltage: 100 VAC to 240 VAC; 50/60 Hz | | | |
| Input DC voltage | | Rated voltage: –48 VDC to –60 VDC | | | |
| Max power | | 350W | | 350W | |
| Operating temperature | | 0°C to 40°C (32°F to 104°F) | | | |
| Relative humidity (noncondensing) | | 5% to 90% | | | |
| Processor | | PowerPC | | PowerPC | |
| BootROM | | 4MB | | 4MB | |
| Memory | | DDR SDRAM:<br>Default: 512MB<br>Max: 1GB | DDR SDRAM II:<br>Default: 1GB<br>Max: 2GB | DDR SDRAM:<br>Default: 512MB<br>Max: 1GB | DDR SDRAM II:<br>Default: 1GB<br>Max: 2GB |
| CF CARD | | Default: 256MB<br>Max: 1GB | | Default: 256MB<br>Max: 1GB | |
| External module | SIC module | 4 | 0 | 4 | 0 |
| | FIC module | 4 | | 6 | |
| | MSCA module | 1 | | 1 | |
| Internal module | ESM module | 2 | | 2 | |
| | VCPM module | 1 | | 1 | |
| | VPM strip | 4 | 0 | 4 | 0 |
| Fixed interface | Console | 1 | | 1 | |
| | AUX | 1 | | 1 | |
| | USB | 2 | | 2 | |
| | FE switching interface | 0 | | 0 | |
| | GE | 2 COMBO | 3 COMBO | 2 COMBO | 3 COMBO |

| | | | | |
|---|---|---|---|---|
| | interfaces | interfaces | interfaces | interfaces |

Table 9 A-MSR 9XX Series Hardware Features

| Item | | A-MSR 900 Description | A-MSR 920 Description |
|---|---|---|---|
| Dimensions (H x W x D) | | 44.2 mm×230 mm×160 mm | 44.2 mm×230 mm×160 mm |
| Weight | | 1.8Kg | 1.8Kg |
| Input AC voltage | | Rated voltage: 100 VAC to 240 VAC; 50/60 Hz | |
| Input DC voltage | | 12V | |
| Max power | | 15W | 15W |
| Operating temperature | | 0～40℃ | |
| Relative humidity (noncondensing) | | 5～90% NO Dew | |
| Processor | | PowerPC | PowerPC |
| BootROM | | 2MB | 2MB |
| Memory | | 256MB | 256MB |
| FLASH | | 256MB | 256MB |
| External module | SIC module | 0 | 0 |
| | MIM module | 0 | 0 |
| Internal module | ESM module | 0 | 0 |
| | VPM strip | 0 | 0 |
| Fixed interface | Console/ AUX | 1 | 1 |
| | USB | 1 | 1 |
| | FE switching interface | 4 | 8 |
| | FE | 2 | 2 |

Table 10 A-MSR20_A-MSR30_A-MSR50_A-MSR900 series Module List

| Module | Description |
|---|---|
| SIC | Ethernet interface cards:<br>JD573B HP A-MSR 4-port 10/100Base-T Switch SIC Module<br>JD620A HP A-MSR 4-port 10/100Base-T PoE Switch SIC Module<br>JD545B HP A-MSR 1-port 10/100Base-T SIC Module<br>JF280A HP A-MSR 1-port 100Base-X SIC Module |

| | |
|---|---|
| | JD572A HP A-MSR 1-port GbE Combo SIC Module<br>JD634B HP A-MSR 1-port E1/Fractional E1 (75ohm) SIC Module<br>JD538A HP A-MSR 1-port T1/Fractional T1 SIC Module<br>JF842A HP A-MSR 2-port E1/Fractional E1 (75ohm) SIC Module<br>JD557A HP A-MSR 1-port Enhanced Sync/Async Serial SIC Module<br>JD536A HP 1-Port Analog Modem SIC A-MSR Module<br>JD537A HP A-MSR 1-port ADSL over POTS SIC Module<br>JD570A HP A-MSR 1-port ISDN-U SIC Module<br>JD571A HP A-MSR 1-port ISDN-S/T SIC Module<br>JF281A HP A-MSR 8-port Async Serial SIC Module<br>JF819A HP A-MSR 802.11b/g/n Wireless Access Point SIC Module<br>JF820A HP 3G Wireless GSM/WCDMA WAN SIC Module<br>JG211A HP A-MSR 802.11b/g/n Wireless Access Point SIC Module (NA)<br>JG056B HP A-MSR 1-port ADSL over ISDN SIC Module<br>JG186A HP A-MSR 16-port Async Serial SIC Module<br>JF253B HP A-MSR 1-port E1/CE1/PRI SIC Module<br>JG187A HP A-MSR HSPA/WCDMA SIC Module<br>Voice interface cards:<br>JD558A HP A-MSR 2-port FXO SIC Module<br>JD559A HP A-MSR 1-port FXO SIC Module<br>JD560A HP A-MSR 2-port FXS SIC Module<br>JD561A HP A-MSR 1-port FXS SIC Module<br>JD575A HP A-MSR 1-port E1 Voice SIC Module<br>JD576A HP A-MSR 1-port T1 Voice SIC Module<br>JF821A HP A-MSR 2-port ISDN-S/T Voice SIC Module<br>JD632A HP A-MSR 2-port FXS/1-port FXO SIC Module |
| DSIC | JD574B HP A-MSR 9-port 10/100Base-T Switch DSIC Module<br>JD621A HP A-MSR 9-port 10/100Base-T PoE Switch DSIC Module<br>JG189A HP A-MSR 4-port FXS/1-port FXO DSIC Module<br>JG191A HP A-MSR 1-port 8-wire G.SHDSL (RJ45) DSIC Module |
| ESM | JD608A HP A-MSR Advanced Network Data Encryption ESM Module<br>JD609A HP A-MSR Standard Network Data Encryption ESM Module |
| MIM | Ethernet interface cards:<br>JD613A HP A-MSR 2-port 10/100Base-T MIM Module<br>JD551A HP A-MSR 4-port 10/100Base-T MIM Module<br>JD548A HP A-MSR 2-port Gig-T MIM Module<br>JD569A HP 16-Port 10/100 MIM A-MSR Module<br>JD618A HP 16-Port 10/100 POE MIM A-MSR Module<br>JD540A HP A-MSR 2-port Enhanced Sync/Async Serial MIM Module<br>JD541A HP A-MSR 4-port Enhanced Sync/Async Serial MIM Module<br>JD552A HP A-MSR 8-port Enhanced Sync/Async Serial MIM Module<br>JF840A HP A-MSR 8-port Enhanced Async Serial MIM Module<br>JF841A HP A-MSR 16-port Enhanced Async Serial MIM Module<br>JD544A HP A-MSR 2-port E1/CE1/PRI MIM Module |

| | |
|---|---|
| | JD549A HP A-MSR 2-port T1/CT1/PRI MIM Module<br>JD550A HP A-MSR 4-port E1/CE1/PRI MIM Module<br>JD556A HP A-MSR 4-port T1 IMA MIM Module<br>JD563A HP A-MSR 8-port E1/CE1/PRI (75ohm) MIM Module<br>JF255A HP A-MSR 8-port E1/Fractional E1 (75ohm) MIM Module<br>JC159A HP A-MSR 8-port T1/Fractional T1 MIM Module<br>JC160A HP A-MSR 8-port T1/CT1/PRI MIM Module<br>JD628A HP A-MSR 1-port T3/CT3/FT3 MIM Module<br>JD630A HP A-MSR 1-port E3/CE3/FE3 MIM Module<br>JD624A HP A-MSR 1-port OC-3c/STM-1c ATM SFP MIM Module<br>JD554A HP NDEC2 Encryption Accel MIM A-MSR Module<br>JD547A HP A-MSR 1-port 4-Wire G.SHDSL MIM Module<br>JG193AHP A-MSR 1-port OC-3c/STM-1c POS MIM Module<br>JF254B HP A-MSR 4-port T1/Fractional T1 MIM Module<br>JF257B HP A-MSR 4-port E1/Fractional E1 MIM Module<br>JD555B HP A-MSR 8-p E1 IMA (75ohm) MIM Module<br>Voice interface card:<br>JD543A HP A-MSR 2-port FXO MIM Module<br>JD542A HP A-MSR 4-port FXO MIM Module<br>JD553A HP A-MSR 4-port FXS MIM Module<br>JD565A HP A-MSR 1-port E1 Voice MIM Module<br>JD566A HP A-MSR 1-port T1 Voice MIM Module<br>JD567A HP A-MSR 2-port E1 Voice MIM Module<br>JD568A HP A-MSR 2-port T1 Voice MIM Module<br>JF822A HP A-MSR 16-port FXS MIM Module<br>JF837A HP A-MSR 4-port ISDN-S/T Voice MIM Module<br>JD539A HP A-MSR 4-port E&M MIM Module |
| DMIM | JD564A HP 24-Port 10/100 DMIM A-MSR Module<br>JD619A HP 24-Port 10/100 POE DMIM A-MSR Module |
| XMIM | JF279A HP A-MSR 16-port 10/100Base-T Switch XMIM Module<br>JF276A HP A-MSR 24-port 10/100Base-T Switch XMIM Module |
| VPM / VCPM | JD610A HP A-MSR Voice Co-processing Module<br>JD598A HP A-MSR 32-Channel Voice Processing Module<br>JD599A HP A-MSR 24-Channel Voice Processing Module<br>JD600A HP A-MSR 16-Channel Voice Processing Module<br>JD601A HP A-MSR 8-Channel Voice Processing Module |
| FIC | Ethernet interface cards:<br>JD583B HP A-MSR 1-port Gig-T FIC Module<br>JF260B HP A-MSR 8-port Enhanced Async Serial FIC Module<br>JF265B HP A-MSR 16-port Enhanced Async Serial FIC Module<br>JF269B HP A-MSR 2-port Gig-T FIC Module<br>JF270B HP A-MSR 2-port 1000Base-X FIC Module<br>JD582A HP A-MSR 1-port 1000Base-X FIC Module<br>JD577A HP A-MSR 2-port 10/100Base-T FIC Module |

| | |
|---|---|
| | JF824A HP A-MSR 4-port 10/100Base-T FIC Module<br>JD604A HP 16-Port 10/100 FIC A-MSR Module<br>JD616A HP 16-Port 10/100 POE FIC A-MSR Module<br>JD584A HP A-MSR 4-port Enhanced Sync/Async Serial FIC Module<br>JD580A HP A-MSR 8-port Enhanced Sync/Async Serial FIC Module<br>JD578A HP A-MSR 2-port E1/CE1/PRI FIC Module<br>JD588A HP A-MSR 4-port E1/CE1/PRI FIC Module<br>JD585A HP A-MSR 8-port E1/CE1/PRI (75ohm) FIC Module<br>JD591A HP A-MSR 4-port E1/Fractional E1 FIC Module<br>JD592A HP A-MSR 4-port T1/Fractional T1 FIC Module<br>JD629A HP A-MSR 1-port T3/CT3/FT3 FIC Module<br>JD625A HP A-MSR 1-port E3/CE3/FE3 FIC Module<br>JD589A HP A-MSR 4-port Enhanced ISDN-S/T FIC Module<br>JD622A HP A-MSR 4-port E1 IMA (75ohm) FIC Module<br>JD595A HP A-MSR 1-port T3 ATM FIC Module<br>JD596A HP A-MSR 1-port E3 ATM FIC Module<br>JD633A HP A-MSR 1-port OC-3c/STM-1c ATM SFP FIC Module<br>JD581C HP A-MSR 1-port OC-3c/STM-1c POS FIC Module<br>JG201A HP A-MSR 1-port OC-3/STM-1 (E1/T1) CPOS FIC Module<br>JD586B HP A-MSR 8-port T1/CT1/PRI FIC Module<br>JG200A HP A-MSR 8-port T1 IMA FIC Module<br>JF278B HP A-MSR 8-p E1 IMA (75ohm) FIC Module<br>Voice interface cards:<br>JD602A HP A-MSR 4-port E&M FIC Module<br>JD593A HP A-MSR 4-port FXO FIC Module<br>JD594A HP A-MSR 4-port FXS FIC Module<br>JD605A HP A-MSR 1-port T1 Voice FIC Module<br>JD606A HP A-MSR 2-port T1 Voice FIC Module<br>JD607A HP A-MSR 1-port E1 Voice FIC Module<br>JD587A HP A-MSR 2-port E1 Voice FIC Module<br>JG197A HP A-MSR 24-port FXS FIC Module |
| D-FIC | JD603A HP 24-Port 10/100 DFIC A-MSR Module<br>JD617A HP 24-Port 10/100 POE DFIC A-MSR Module |

CAUTION:

The support and restriction of modules on A-MSR please refer to HP A-MSR Router Series Interface Module Guide, Appendix Purchase Guide.

# Software features

Table 11 Software features of A-MSR20_A-MSR30_A-MSR50_A-MSR900 Series

| Category | Features |
|---|---|
| LAN protocol: | ARP (proxy ARP, free ARP, authorization ARP)<br>Ethernet_II<br>Ethernet_SNAP<br>VLAN (PORT-BASED VLAN/MAC-BASED VLAN/VLAN-BASED PORT ISOLATE/VLAN VPN/VOICE VLAN)<br>802.3x<br>LACP(802.3ad)<br>802.1p<br>802.1Q<br>802.1x<br>RSTP(802.1w)<br>MSTP(802.1s)<br>GVRP<br>PORT MUTILCAST suppression |
| WAN protocols: | PPP, MP<br>PPPoE Client, PPPoE Server<br>PPP/MP over FR<br>FR, MFR<br>FR Fragment, FR Compress, FR over IP<br>FRTS<br>ATM(IPoA, IPoEoA, PPPoA, PPPoEoA)<br>DCC, Dialer Watch<br>HDLC<br>LAPB<br>X25, X25 over TCP, X25 to TCP<br>X25 PAD, X25 Huntgroup, X25 CUG<br>DLSW(V1.0/2.0)<br>ISDN, ISDN Network<br>ISDN QSIG<br>MODEM |
| IP services | Fast forwarding (unicast/multicast)<br>TCP<br>UDP<br>IP Option<br>IP unnumber<br>Policy routing (unicast/multicast) |
| Non-IP services: | SNA/DLSw support<br>DLSw Ethernet redundancy backup |

| | |
|---|---|
| | IPX |
| | Netstream |
| IP application | Ping and Trace |
| | DHCP Server |
| | DHCP Relay |
| | DHCP Client |
| | DNS client |
| | DNS Static |
| | NQA |
| | IP Accounting |
| | UDP Helper |
| | NTP |
| | Telnet |
| | TFTP Client |
| | FTP Client |
| | FTP Server |
| IP route | Static routing management |
| | Dynamic routing protocols: |
| | RIP/RIPng |
| | OSPF |
| | OSPFv3 |
| | BGP |
| | IS-IS |
| | Multicast routing protocols: |
| | IGMP |
| | PIM-DM |
| | PIM-SM |
| | MBGP |
| | MSDP |
| | Routing policy |
| MPLS | LDP |
| | LSPM |
| | MPLS TE |
| | MPLS FW |
| | MPLS/BGP VPN |
| | L2VPN |
| IPv6 | IPv6 basic functions |
| | IPv6 ND |
| | IPv6 PMTU |
| | IPv6 FIB |
| | IPv6 ACL |
| | IPv6 transition technologies |
| | NAT-PT |
| | IPv6 tunneling |

| | |
|---|---|
| | 6PE |
| | IPv6 routing |
| | IPv6 static routing management |
| | Dynamic routing protocols |
| | RIPng |
| | OSPFv3 |
| | IS-ISv6 |
| | BGP4+ |
| | Multicast routing protocols |
| | MLD |
| | PIM-DM |
| | PIM-SM |
| | PIM-SSM |
| Port security | PPPoE Client&Server |
| | PORTAL |
| | 802.1x |
| AAA | Local authentication |
| | Radius |
| | HWTacacs |
| Firewall | ASPF |
| | ACL |
| | FILTER |
| | DDOS |
| Data security | IKE |
| | IPSec |
| | Encryption card |
| | Portal/Portal+ |
| Other security technologies | L2TP |
| | NAT/NAPT |
| | PKI |
| | RSA |
| | SSH V1.5/2.0 |
| | SSL (only support cooperate with CWMP) |
| | URPF |
| | GRE |
| | DVPN |
| Reliability | Supports VRRP |
| | Supports the backup center |
| L2 QoS | SP |
| | WRED(Port) |
| | CAR |
| | LR |
| | Flow-base QOS Policy |

| | |
|---|---|
| | Port-Based Mirroring<br>Flow-Based Mirroring<br>Cos-Based HOLB(Head of Line Blocking)Prevention<br>Packet Remarking<br>Flow Redirect<br>Flow Accounting<br>Priority Mapping<br>Port Trust Mode<br>Port Priority<br>Flow Filter<br>FlowControl<br>ACL |
| Traffic supervision | Supports CAR (Committed Access Rate)<br>Supports LR (Line Rate) |
| Congestion management | FIFO, PQ, CQ, WFQ, CBQ, RTPQ |
| Congestion avoidance | WRED/RED |
| Traffic shaping | Supports GTS(Generic Traffic Shaping) |
| Other QOS technologies | FR QOS<br>MPLS QOS<br>MP QoS/LFI<br>cRTP/IPHC<br>ATM QOS<br>Sub-interface QOS |
| Voice Interfaces | FXS<br>FXO<br>E&M<br>E1VI/T1VI |
| Voice Signaling | R2<br>DSS1<br>Q.sig<br>Digital E&M |
| SIP | SIP<br>SIP Operation |
| Codec | G.711A law<br>G.711U law<br>G.723R53<br>G.723R63<br>G.729a<br>G.729R8 |
| Media Process | RTP/cRTP<br>IPHC |

| | |
|---|---|
| | Voice Backup |
| FAX | FAX |
| Other | Voice RADIUS<br>VoFR<br>Analog voice access and emergency |
| Network management | SNMP V1/V2c/V3<br>MIB<br>SYSLOG<br>RMON |
| Local management | Command line management<br>File system management<br>Dual Image |
| User access management | Supports console interface login<br>Supports AUX interface login<br>Supports TTY interface login<br>Supports telnet (VTY) login<br>Supports SSH login<br>Supports FTP login<br>Supports X25 PAD login<br>XMODEM |

# Version updates

# Feature updates

Table 12 Feature updates

| Item | Description |
|---|---|
| CMW520-R2209 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New features:<br>1. CWMP support for configuring multiple ACS servers.<br>2. Support multicast UDPH function<br>At the last hop of multicast transmitting, the multicast UDPH function can transfer multicast packets to broadcast packets.<br>3. Support to using the sub-address of the interface sending and receiving RIP routes<br>Deleted features: None<br>Modified features: None |

| Item | Description |
| --- | --- |
| CMW520-R2207P45 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New features:<br>1. Using the command of "impedance south-africa" to set the FXO interface's ringing impedance<br>2. Support HUAWEI EC1261 3G modem<br>3. If The NAT and IPSEC functions were enabled at the same interface, the command of "ipsec no-nat-process enable" can control that packets don't do NAT transition before IPSEC<br>4. Support of CWMP over AES-256 SSL tunnel<br>5. Support of CWMP (TR-069) over SSL for BIMS and the router<br>Deleted features: None<br>Modified features: None |
| CMW520-R2207P38 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New features:<br>1. The MIM-G.SHDSL and FIC-G.SHDSL card supported the Whip function<br>Deleted features: None<br>Modified features: None |
| CMW520-R2207P34 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New features:<br>1. Support Huawei E261 3G modem and ZTE MF190 3G modem<br>Deleted features: None<br>Modified features: None |
| CMW520-R2207P23 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New Features:<br>1. Delay to notify the status change of interface<br>2. Support to encrypt HWTACAS Key<br>3. The Statistic information of the MFR main interface included the input and output packets from sub-interface. |
| CMW520-R2207P14 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New Features: |

| Item | Description |
| --- | --- |
| | 1. The number of NAT address pool was extended to 64 from 32.<br>2. Support Sierra 250U and 308U 3G modem at the A-MSR20/A-MSR30/A-MSR9XX router.<br>3. Support HUAWEI E173 WCDMA modem<br>4. Support to Configure TPID on a Layer 3 Ethernet or VE interface, and to implement VLAN termination.<br>5. Support to transit the extendedVideoCapability field of H245 packets in the NAT ALG<br>6. Support the DVPN instance.<br>7. The QoS policy of main interface can apply to sub-interface.<br>If there wasn't QoS policy at the sub-interface, the QoS policy of main interface could apply to sub-interface.<br>8. Support the Refer-by field of the SIP packets. |
| CMW520-R2207P02 | |
| Hardware feature updates | New features: None<br>Deleted features: None |
| Software feature updates | New features:<br>1. Support the statistics per classifier of nested QoS<br>Deleted features: None<br>Modified features: None |
| CMW520-R2207 | |
| Hardware feature updates | None |
| Software feature updates | New features:<br>1. Call forwarding authority control<br>When performing call forwarding, the system checks both the calling number and the called number. If either of them is authorized to call the forwarded-to number, the call can be forwarded.<br>2. Support DAR MIB<br>The statistics of the packets for the DAR can be acquired by the MIB.<br>3. Authorization again for AAA<br>For AAA scheme, if the device prompts you to enter another password of the specified type after you entering the correct username and password, you will be authenticated for the second time. In other words, to pass authentication, you must enter a correct password as prompted.<br>4. The feature supports the VPN could visit the other VPN by NAT<br>5. Support OSPF and NAT in bridge-template interface<br>6. WCDMA 3G Modem<br>Huawei E170/E172/E226/E160/E169/E176/E156/E180/E1750/E176G /E1756/E1556/K3765/K4505/E1820/E367/E1553 (E226 is only supported on MSR30/MSR50 routers)<br>7. CDMA2000 3G Modem<br>Huawei EC226/EC169/EC1260/EC1261; ZTE AC2726; VTION |

| Item | Description |
| --- | --- |
| | E1916<br>8. TD-SCDMA 3G Modem<br>Huawei ET128/ET188/ET127<br>9. SIP TRUNKING<br>As more enterprise IP-PBX networks run SIP and more Internet Telephone Service Providers (ITSPs) use SIP to provide basic voice communication structures, enterprises urgently need a technology that can connect the enterprise IP-PBX network to the ITSP over SIP. This technology is called SIP trunk. The SIP trunk function can be embedded into the voice gateway or the firewall deployed at the network edge. The device providing the SIP trunk function is called the SIP trunk device, or the SIP trunk gateway (TG).<br>10. SRTP<br>As an enhancement of RTP, SRTP secures RTP packets through authentication, encryption, and integrity check. It can encrypt media packets between two SIP terminals. SIP TLS is used to encrypt audio and video signaling streams.<br>11. L2VPN connected to L3VPN<br>An MPLS L2VPN can be used as an access network to connect users to an MPLS L3VPN or IP backbone. The conventional solution needs two devices to complete this task. This feature enables a single device to implement this function to reduce networking costs and complexity.<br>12. NAT DMZ host and related features<br>1) After you configure an internal server, NAT gives precedence to the service provided by the internal server.<br>2) Allow LAN users to access the internal server by using a public network destination address and a port number.<br>3) Allow you to configure the NAT DMZ host through web.<br>13. SIP support for non early media negotiation<br>With this feature, a router that acts as the called party can send a 180 ringing response without media information to the calling party so that the calling party receives only tones played by the server.<br>14. IPsec RRI<br>IPsec Reverse Route Inject (RRI) enables an IPsec tunnel gateway to automatically add static routes destined for protected private networks or peer IPsec tunnel gateways to a routing table.<br>The next hop of the static routes specifies the IPsec tunnel peer. If it specifies the peer IPsec VPN gateway, traffic sent to the gateway is protected by IPsec.<br>15. Allows you to configure NAT address groups, NAT server, and attack protection through TR069.<br>16. Support of routing protocols for 6VPE<br>Add the IPv6 VPN feature and enable BGP, ISIS, and RIPng to support IPv6 VPN.<br>17. BIDIR-PIM<br>In some many-to-many applications, such as multi-side video conference, there might be multiple receivers interested in |

| Item | Description |
| --- | --- |
| | multiple multicast sources simultaneously. With PIM-DM or PIM-SM, each router along the SPT must create an (S, G) entry for each multicast source, consuming a lot of system resources.<br>BIDIR-PIM addresses the problem. Derived from PIM-SM, BIDIR-PIM builds and maintains bidirectional RPTs, each of which is rooted at an RP and connects multiple multicast sources with multiple receivers. Traffic from the multicast sources is forwarded through the RPs to the receivers along the bidirectional RPTs. Each router needs to maintain only one (*, G) multicast routing entry, saving system resources.<br>BIDIR-PIM is suitable for networks with dense multicast sources and dense receivers.<br>18. OSPFv3 support for MCE<br>With MCE, you can bind each VPN to a VLAN interface on a CE device. The CE creates and maintains a separate routing table (multi-VRF) for each VPN. This separates the forwarding paths of packets of different VPNs and, in conjunction with the PE, can correctly advertise the routes of each VPN to the peer PE, ensuring the normal transmission of VPN packets over the public network.<br>19. Voice support for TR104<br>TR104 specifies a list of objects and nodes a CPE device that acts as a VoIP endpoint should have and support. This feature supports some nodes in the list.<br>20. BGP, OSPFv3 and ISISv6 support for IPv6 VPN BFD<br>Use BFD to detect links between IPv6 routing protocol neighbors to speed up network convergence.<br>21. Allows you to set a BGP update interval of 0.<br>22. Allows you to use domain names to specify SNMP trap and log hosts.<br>23. TR069 supports the following memory and CPU utilization nodes:<br>InternetGatewayDevice.DeviceInfo.X_CT-COM_LoadInfo.ProcessorLoad<br>InternetGatewayDevice.DeviceInfo.X_CT-COM_LoadInfo.MemoryLoad<br>24. ACL configuration information display filtering<br>Allows you to use command parameters to filter specific ACL configuration information in the display command output.<br>25. A routing policy name can contain up to 64 characters.<br>26. Allows you to use names as BGP community attributes<br>27. Permanent attribute for static routes<br>Allows you to set a static route as a permanent static route. A permanent static route is active even when its output interface is down.<br>28. Continue feature for routing policy<br>With this feature, a route that has matched the current policy node is matched against the next policy node. This feature enables you combine the if-match and apply clauses of policy nodes as needed to increase routing policy flexibility. |

| Item | Description |
| --- | --- |
| | 29. E1POS and AM ports can send calling numbers.<br>30. POS terminal access can use the source address in the TPDU header to map POS packets to specific POS applications.<br>31. POS terminal access allows you to specify TCP source port numbers for POS applications.<br>32. Bloomberg MSR Source NAT<br>In NAT NOPAT mode (NOPAT dynamic entries exist), this feature provides ACL-based filtering for connections initiated from the external network to the internal network and for statically NATed connections.<br>33. NAT support for discontinuous address pools<br>34. ISDN support for sending the progress-indicator unit<br>You can use the isdn progress-indicator command to configure the ISDN signaling packets to carry the progress indicator unit and set the value of the unit.<br>35. An ACL name can contain up to 63 characters.<br>36. POS MIB and E1 POS MIB<br>37. SIP support for SRV and NAPTR<br>Enables the router to use SRV and NAPTR to perform domain name resolution during SIP calls and registrations. This feature also supports call failure triggered registrations and server keep-alive function.<br>38. TR098 |
| CMW520-R2105P38 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support FRF.12 fragment function based on the interface<br>2. FIPS features appended<br>1) Perform Self-Tests: Initiate and run the self-test as specified in standard.<br>2) Support to calculate the abstract of the application software<br>3) The decrypt known answer tests for the symmetric cryptographic algorithms (AES and Triple-DES).<br>4) Support a Continuous Random Number Generator Test for encryption engine. |
| CMW520-R2105P35 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support the statistics per classifier of nested QoS |
| CMW520-R2105P31 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support the packets and the rate Statistic at the vlan-interface<br>2. Set the number of interframe filling tag using the command |

| Item | Description |
| --- | --- |
| | The default number of interframe filling tag was four, and in order to improve the utilization of the interface bandwidth the router added the command of "itf number" to set the number of interframe filling tag.<br>3. Support to assign the IP address of next server offering service for the DHCP client |
| CMW520-R2105P25 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support FIPS. |
| CMW520-R2105P22 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support to set virtual bandwidth using the command of "bandwidth" at the interface.<br>2. At best every VRF can support 10000 routes at the MSR50 router. |
| CMW520-R2105P12 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support HUAWEI E367 models of WCDMA 3G Modems.<br>2. MSR50 MPU-G2 can support 10000 rules each ACL.<br>3. Support remarking the protocol packets from the router itself. |
| CMW520-R2105P06 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support HUAWEI E1553 models of WCDMA 3G Modems.<br>2. IPv6 capabilities in VPNs<br>It supports IPV6 capabilities in VPNs that run on the route protocol such as BGP, ISIS and RIPING.<br>3. Support LLDP in LAN<br>It supports LLDP protocol (Link Layer Discovery Protocol) in LAN interface. |
| CMW520-R2105P02 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Excluding the ACL information when displaying current configuration<br>When displaying the current configuration the feature supports to move the Acl information by adding the "exclude" parameter.<br>2. It can be enlarged to 64 characters for the route-policy name, a case-sensitive string of 1 to 63 characters.<br>3. It can put a name to describe the BGP community lists, a |

| Item | Description |
|---|---|
| | string of 1 to 31 characters (not all are numbers).<br>4. Permanent Static Route<br>It will keep activation even if the outbound interface becomes down when configuring the permanent static route. |
| CMW520-R2105 | |
| Hardware feature updates | None |
| Software feature updates | New Features:<br>1. Support HUAWEI E1820 models of WCDMA 3G Modem<br>2. BIDIR-PIM<br>In some many-to-many applications, such as multi-side video conference, there may be multiple receivers interested in multiple multicast sources simultaneously. With PIM-DM or PIM-SM, each router along the SPT must create an (S, G) entry for each multicast source, consuming a lot of system resources. BIDIR-PIM is introduced to address this problem. Derived from PIM-SM, BIDIR-PIM builds and maintains bidirectional RPTs, each of which is rooted at an RP and connects multiple multicast sources with multiple receivers. Traffic from the multicast sources is forwarded through the RP to the receivers along the bidirectional RPT. In this case, each router needs to maintain only a (*, G) multicast routing entry, saving system resources.<br>BIDIR-PIM is suitable for networks with dense multicast sources and dense receivers. |

# Command line updates

Table 13 Command line updates

| Item | Description |
|---|---|
| CMW520-R2209 | |
| New commands | 1. Syntax<br>**parameter auto-select** { **save** \| **load** \| **remove** *calling-number* **}**<br>Views<br>e1pos-adaptor view<br>Parameters<br>save: Saves the automatically selected parameter groups to a file named e1pos_para.rec.<br>load: Reads the parameter groups from the file into the router memory.<br>remove *calling-number*: Removes the previous selection for a calling number to reselect a parameter group for the next call.<br>Description<br>Use parameter auto-select to save, read, or delete automatically selected parameter groups.<br>Examples<br># Save automatically selected parameter groups. |

| Item | Description |
| --- | --- |
| | <Sysname> system-view<br>[Sysname] e1pos-adaptor<br>[Sysname-e1pos-adaptor] parameter auto-select save<br>parameter auto-select enable<br>2.Syntax<br>**parameter auto-select enable**<br>**undo parameter auto-select enable**<br>Views<br>e1pos-adaptor view<br>Description<br>Use parameter auto-select enable to enable automatic selection of negotiation parameter groups.<br>Use undo parameter auto-select enable to restore the default.<br>By default, automatic selection of negotiation parameter groups is enabled.<br>Examples<br># Enable automatic selection of negotiation parameter groups.<br><Sysname> system-view<br>[Sysname] e1pos-adaptor<br>[Sysname-e1pos-adaptor] parameter auto-select enable<br>3.Syntax<br>**udp-helper multicast-map** *multicast-address broadcast-address* [ **acl** *acl-number* ]<br>**undo udp-helper multicast-map** *multicast-address broadcast-address*<br>View<br>Interface view<br>Parameters<br>*multicast-address*: Specifies the destination multicast address of the UDP multicast packets to be forwarded by UDP helper.<br>*broadcast-address*: Specifies the subnet broadcast address.<br>acl *acl-number*: Specifies an ACL for identifying UDP multicast packets. UDP helper processes the packets matching the permit rule in the ACL. The *acl-number* argument is in the range of 2000 to 2999 for a basic ACL, or 3000 to 3999 for an advanced ACL.<br>Description<br>Use udp-helper multicast-map to configure the mapping between a multicast address and a subnet broadcast address. Upon receiving a matching UDP multicast packet, UDP helper converts its destination multicast address into the specified subnet broadcast address.<br>Use undo udp-helper multicast-map to remove the mapping between a multicast address and a subnet broadcast address.<br>Configure multicast address-to-subnet broadcast address mapping on the interface that receives UDP multicast packets.<br>You can configure up to 50 multicast address-to-subnet broadcast address mappings on an interface.<br>Examples<br># Configure a mapping between a multicast address and a subnet |

| Item | Description |
| --- | --- |
| | broadcast address on Ethernet 1/1.<br><Sysname> system-view<br>[Sysname] interface ethernet 1/1<br>[Sysname-Ethernet1/1] udp-helper multicast-map 224.1.1.1 192.168.3.255 |
| Removed commands | None |
| Modified commands | 1.<br>Original command:<br>**parameter-group** *group-number*<br>**undo parameter-group {** *group-number* \| **all }**<br>Modified command:<br>parameter-group group-number<br>undo parameter-group { group-number \| all }<br>Module of the command: POS terminal access<br>Description: Add automatic selection to group-number: Specifies a group number, in the range of 1 to 128 for maunal configuration and 129 to 144 for automatic selection..<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.<br>Original command:<br>**rta terminal** *template-name terminal-number*<br>**undo rta terminal**<br>Modified command:<br>**rta terminal** *template-name terminal-number* **[ backup ]**<br>**undo rta terminal**<br>Module of the command: Terminal access<br>Description: Add a new parameter of [ backup ].<br>backup: Specifies the interface as a backup interface.<br>Use the rta terminal command to apply a template on the interface.<br>Use the undo rta terminal command to cancel the template application.<br>By default, no template is applied on the interface.<br>An interface can use only one template, but a template can be applied to multiple interfaces. If multiple interfaces use one template, the interface not configured with the backup keyword serves as the primary interface, and the interface configured with the backup keyword serves as the backup interface.<br>The system detects the primary interface every five seconds. If one of the following situations occurs, the system changes the backup interface to the primary interface, and the original primary interface becomes a backup interface. The system detects the new primary interface in the same way.<br>The primary interface does not receive data within five seconds. |

| Item | Description |
| --- | --- |
| | The primary interface receives five or more CRC error packets within five seconds.<br>The primary interface goes down.<br>NOTE: Data loss might occur during a primary/backup switchover.<br>A terminal can be created only after the configured template is applied on the corresponding interface. Use the terminal-number argument to specify the terminal number. An interface can be connected to only one physical terminal. The router identifies physical terminals by terminal number.<br>At least one VTY should be configured in the terminal template for the template to be applied on the interface. This command supports asynchronous serial interfaces, synchronous/asynchronous serial interfaces, and AUX interfaces. When a synchronous/asynchronous serial interface operates in the synchronous mode, you can configure only RTC terminal access on the interface. When a synchronous/asynchronous serial interface operates in the asynchronous mode, you can configure all access types except UDP-based RTC on the interface.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>3.<br>Original command:<br>**firewall packet-filter ipv6 {** *acl6-number* \| *name acl6-name* **} { inbound** \| **outbound }**<br>**undo firewall packet-filter ipv6 [ {** *acl6-number* \| *name acl6-name* **} ] { inbound** \| **outbound }**<br>Modified command:<br>**firewall packet-filter ipv6 {** *acl6-number* \| *name acl6-name* **} { inbound** \| **outbound }**<br>**undo firewall packet-filter ipv6 [ {** *acl6-number* \| *name acl6-name* **} ] { inbound** \| **outbound }**<br>Module of the command: Firewall<br>Description: Add an Ethernet frame header ACL to acl6-number:<br>acl-number: Specifies an IPv6 ACL by its number, which is in the range of 2000 to 2999 for an IPv6 basic ACL, 3000 to 3999 for an IPv6 advanced ACL, or 4000 to 4999 for an Ethernet frame header ACL.<br>name acl6-name: Specifies an IPv6 basic ACL, an Ethernet frame header ACL, or an IPv6 advanced ACL by its name. The acl6-name argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be all.<br>Changes in default values: None.<br>Changes in value ranges: None. |
| CMW520-R2207P45 | |
| New commands | 1. Syntax<br>**ipsec no-nat-process enable**<br>**undo ipsec no-nat-process enable**<br>View |

| Item | Description |
| --- | --- |
| | Interface view<br>Parameters<br>None<br>Description<br>Use the ipsec no-nat-process enable command to configure the interface to forward packets to IPsec transparently without performing address translation.<br>Use the undo ipsec no-nat-process enable command to restore the default.<br>By default, if both NAT and IPsec are configured on an interface, outgoing packets on the interface will be processed by NAT and then by IPsec.<br>Configure this command if you require that packets to be protected by IPsec not to be NATed.<br>Examples<br># Configure interface Ethernet 0/0 to forward packets to IPsec transparently without performing address translation.<br><Sysname> system-view<br>[Sysname] interface ethernet 0/0<br>[Sysname-Ethernet0/0] ipsec no-nat-process enable |
| Removed commands | None |
| Modified commands | 1.<br>Original command:<br>**impedance { *country-name* \| r550 \| r600 \| r650 \| r700 \| r750 \| r800 \| r850 \| r900 \| r950 }**<br>**undo impedance**<br>Modified command:<br>**impedance { *country-name* \| r550 \| r600 \| r650 \| r700 \| r750 \| r800 \| r850 \| r900 \| r950 }**<br>**undo impedance**<br>Module of the command: Voice Subscriber Line<br>Description: Add a new country to the new parameter of ***country-name***: South-Africa.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.<br>Original command:<br>**dot1x timer { handshake-period *handshake-period-value* \| quiet-period *quiet-period-value* \| reauth-period *reauth-period-value* \| server-timeout *server-timeout-value* \| supp-timeout *supp-timeout-value* \| tx-period *tx-period-value* }**<br>Modified command:<br>**dot1x timer { handshake-period *handshake-period-value* \| quiet-period *quiet-period-value* \| reauth-period *reauth-period-value* \| server-timeout *server-timeout-value* \| supp-timeout *supp-timeout-value* \| tx-period** |

| Item | Description |
| --- | --- |
| | ***tx-period-value* }**<br>Module of the command: 802.1X<br>Description: Chang the range of *reauth-period-value* from 60～7200 to 60～86400.<br>Changes in default values: None.<br>Changes in value ranges: None. |
| CMW520-R2207P38 | |
| New commands | 1. Syntax<br>**cable { long { 0db \| -7.5db \| -15db \| -22.5db } \| short { 133ft \| 266ft \| 399ft \| 533ft \| 655ft } }**<br>**undo cable**<br>View<br>ATM T1 interface view<br>Parameters<br>long: Matches 199.6-meter (655-feet) and longer cable length. The options for this parameter include 0db, -7.5db, -15db and -22.5db. The attenuation parameter is selected depending on the signal quality received at the receiving end. No external CSU is needed.<br>short: Matches a cable length shorter than 199.6 meters (655 feet). The options for this parameter include 133ft, 266ft, 399ft, 533ft and 655ft. The *length* parameter is selected depending on the actual transmission distance.<br>Description<br>Use the cable command to set the cable attenuation and length on the ATM T1 interface.<br>Use the undo cable command to restore the default, long 0db.<br>You may use this command to adapt signal waveform to different transmission conditions such as the quality of the signal received by the receiver. If the signal quality is good, you can use the default setting. The ATM T1 interface does not need an external CSU device.<br>Examples<br># Set the cable length to 40.5 meter (133 feet) on ATM T1 interface 1/0.<br><Sysname> system-view<br>[Sysname] interface atm 1/0<br>[Sysname-Atm1/0] cable short 133ft |
| Removed commands | None |
| Modified commands | 1.<br>Original command:<br>**display transceiver { controller [** *controller-type controller-number* **] \| interface [** *interface-type interface-number* **] } [ \| { begin \| exclude \| include }** *regular-expression* **]**<br>Modified command:<br>**display transceiver { controller [** *controller-type controller-number* **] \| interface [** *interface-type interface-number* **] } [ \| { begin \| exclude \| include }** *regular-expression* **]** |

| Item | Description |
|---|---|
| | Module of the command: Device Management<br>Description:<br>Add the new output information for this command:<br>Info: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.<br>Changes in default values: None.<br>Changes in value ranges: None. |
| CMW520-R2207P34 | |
| New commands | 1. Syntax<br>**rip bfd enable destination** *ip-address*<br>**undo rip bfd enable**<br>View<br>Interface view<br>Parameters<br>ip-address: IP address of a neighbor.<br>Description<br>Use the rip bfd enable destination command to enable BFD for a directly connected neighbor.<br>Use the command to restore the default and remove the BFD session to the neighbor. Use the undo rip bfd enable destination command to resteore the default.<br>By default, BFD is not enabled for any neighbor.<br>When the link to the specified neighbor fails, the interface connected to the neighbor stops advertising RIP messages. When the link recovers, the interface starts to advertise RIP messages.<br>Note: This command cannot be used together with the rip bfd enable command.<br>Examples<br># Enable BFD for the neighbor 202.38.165.1 on Ethernet1/1.<br><Sysname> system-view<br>[Sysname] interface ethernet 1/1<br>[Sysname-Ethernet1/1] rip bfd enable destination 202.38.165.1 |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2207P23 | |
| New commands | 1. Syntax<br>**link-delay** *delay-time*<br>**undo link-delay**<br>View<br>E1-F interface view, T1-F interface view, CE3 interface view, CT3 interface view, CE1/PRI interface view, CT1/PRI interface view |

| Item | Description |
| --- | --- |
| | Parameters<br>*delay-time*: Sets the physical state change suppression interval (in seconds), which ranges from 0 to 10. The value of 0 disables physical state change suppression (which can also be disabled by using the undo link-delay command) on a WAN interface.<br>Description<br>Use the link-delay command to set the physical state change suppression interval on a WAN interface.<br>Use the undo link-delay command to restore the default.<br>By default, physical state change suppression is disabled on a WAN interface. The system detects the physical state changes of interfaces every 5 seconds. When a physical state change occurs, the system will detect the change within 5 seconds and immediately report the detected change.<br>Suppose you set the *delay-time* argument to a value ranging from 1 to 10, for example, 2, for an interface. When a physical state change occurs to the interface, the system will detect the change within 5 seconds after the change and report the change 2 seconds after detecting the change, in other words, the system will report the change 2 to 7 seconds after the change.<br>For a CE3, CT3, CE1/PRI, or CT1/PRI interface, you must execute this command in controller view. For an E1-F or a T1-F interface, you must execute this command in the view of the corresponding serial interface. In the view of a serial interface corresponding to any other synchronous/asynchronous interface, this command is not available.<br>Note: This command does not apply to ports administratively shut down (with the shutdown command).<br>Examples<br># Set the physical state change suppression interval to 2 seconds on CE1/PRI interface E1 2/0, so that the system will detect a physical state change on the interface and report the change 2 to 7 seconds after the change.<br><Sysname> system-view<br>[Sysname] controller e1 2/0<br>[Sysname-E1 2/0] link-delay 2<br>2. Syntax<br>**link-delay** *delay-time*<br>**undo link-delay**<br>View<br>VE1/VT1 interface view<br>Parameters<br>*delay-time*: Sets the physical state change suppression interval (in seconds), which ranges from 0 to 10. The value of 0 disables physical state change suppression (which can also be disabled by using the undo link-delay command) on a VE1/VT1 interface.<br>Description<br>Use the link-delay command to set the physical state change suppression interval on a VE1/VT1 interface.<br>Use the undo link-delay command to restore the default.<br>By default, physical state change suppression is disabled on a VE1/VT1 |

| Item | Description |
| --- | --- |
| | interface. The system detects the physical state changes of interfaces every 5 seconds. When a physical state change occurs, the system will detect the change within 5 seconds after the change and immediately report the detected change.<br>Suppose you set the *delay-time* argument to a value ranging from 1 to 10, for example, 2, for an interface. When a physical state change occurs to the interface, the system will detect the change within 5 seconds after the change and report the change 2 seconds after detecting the change, in other words, the system will report the change 2 to 7 seconds after the change.<br>You must execute this command in controller view.<br>Note: This command does not apply to ports administratively shut down (with the shutdown command).<br>Examples<br># Set the physical state change suppression interval to 2 seconds on VE1/VT1 interface E1 2/0, so that the system will detect a physical state change on the interface and report the change 2 to 7 seconds after the change.<br><Sysname> system-view<br>[Sysname] controller e1 2/0<br>[Sysname-E1 2/0] link-delay 2 |
| Removed commands | None |
| Modified commands | 1.<br>Original command:<br>**key** { **accounting** \| **authentication** \| **authorization** } *key*<br>**undo key** { **accounting** \| **authentication** \| **authorization** }<br>Modified command:<br>**key** { **accounting** \| **authentication** \| **authorization** } [ **cipher** \| **simple** ] *key*<br>**undo key** { **accounting** \| **authentication** \| **authorization** }<br>Module of the command: AAA<br>Description: Add the new parameters of [ **cipher** \| **simple** ] and change the description of *key:*<br>*key*: Shared key, case sensitive. Follow these guidelines:<br>With the cipher keyword specified, the key must be a ciphertext string of 1 to 352 characters, such as _(TT8F]Y\5SQ=^Q`MAF4<1!!.<br>With the simple keyword specified, the key must be a plaintext string of 1 to 255 characters, such as aabbcc.<br>With neither the cipher keyword nor the simple keyword specified, the key must be a plaintext string, and the key will be displayed in cipher text.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.<br>Original command:<br>**link-delay** *delay-time*<br>**undo link-delay**<br>Modified command: |

| Item | Description |
| --- | --- |
| | **link-delay** *delay-time*<br>**undo link-delay**<br>Module of the command: Ethernet<br>Description: Modify the value ranges and description of *delay-time*.<br>*delay-time*: Sets the physical state change suppression interval (in seconds), which ranges from 0 to 10. This argument is 0 or the default value for an Ethernet interface. The value of 0 disables physical state change suppression, and enables the system to promptly detect physical state change on the Ethernet interface.<br>Changes in default values: By default, the system detects the physical state changes of interfaces every 5 seconds. When a physical state change occurs, the system will detect the change within 5 seconds after the change and immediately report the detected change.<br>Changes in value ranges: None. |
| CMW520-R2207P14 | |
| New commands | 1. Syntax<br>**tunnel vpn-instance** *vpn-instance-name*<br>**undo tunnel** vpn-instance<br>View<br>Tunnel interface view<br>Parameters<br>*vpn-instance-name*: Name of an MPLS L3VPN instance, a case-sensitive string of 1 to 31 characters.<br>Description<br>Use the tunnel vpn-instance command to specify the VPN to which the tunnel destination address belongs.<br>Use the undo tunnel vpn-instance command to restore the default.<br>By default, a DVPN tunnel destination address belongs to the public network.<br>After you specify the VPN to which the tunnel destination address belongs by using the tunnel vpn-instance command, the device searches the routing table of the specified VPN instance to forward tunneled packets.<br>You can use the ip binding vpn-instance command on the tunnel's source interface to specify the VPN to which the tunnel source address belongs. The tunnel source address and the tunnel destination address must belong to the same VPN or both belong to the public network.<br>For more information about the ip binding vpn-instance command, see the *MPLS Command Reference*.<br>Examples<br># On interface Tunnel 0, specify the tunneled packets to belong to the VPN vpn10.<br><Sysname> system-view<br>[Sysname] ip vpn-instance vpn10<br>[Sysname-vpn-instance-vpn10] route-distinguisher 1:1<br>[Sysname-vpn-instance-vpn10] vpn-target 1:1<br>[Sysname-vpn-instance-vpn10] quit<br>[Sysname] int ethernet 1/1 |

| Item | Description |
| --- | --- |
| | [Sysname-Ethernet1/1] ip binding vpn-instance vpn10<br>[Sysname-Ethernet1/1] ip address 1.1.1.1 24<br>[Sysname-Ethernet1/1] quit<br>[Sysname] interface tunnel 0<br>[Sysname-Tunnel0] tunnel-protocol dvpn udp<br>[Sysname-Tunnel0] source ethernet 1/1<br>[Sysname-Tunnel0] tunnel vpn-instance vpn10<br>2. Syntax<br>**fr fragment** [ *fragment-size* ] **end-to-end**<br>**undo fr fragment**<br>View<br>FR interface view<br>Parameters<br>*fragment-size*: Fragment size, which ranges from 16 bytes to 1600 bytes. This argument is 45 bytes by default.<br>Description<br>Use the fr fragment command to enable the FRF.12 packet fragmentation function for FR interface.<br>Use the undo fragment command to disable the FRF.12 packet fragmentation function.<br>By default, the FRF.12 packet fragmentation function is disabled for FR interface.<br>You cannot configure this command together with the fr traffic-sharping command.<br>Examples<br># Enable the FRF.12 packet fragmentation function with default fragment size of 45 bytes for the interface Serial2/0.<br><Sysname> system-view<br>[Sysname] interface serial 2/0<br>[Sysname-serial2/0] link-protocol fr<br>[Sysname-serial2/0] fr fragment end-to-end<br># Enable the FRF.12 packet fragmentation function with fragment size of 300 bytes for the interface Serial2/1.<br><Sysname> system-view<br>[Sysname] interface serial 2/1<br>[Sysname-serial2/1] link-protocol fr<br>[Sysname-serial2/1] fr fragment 300 end-to-end<br>3. Syntax<br>**modem auto-recovery enable**<br>**undo modem auto-recovery enable**<br>Views<br>Cellular interface view<br>Parameters<br>None<br>Description |

| Item | Description |
| --- | --- |
| | Use the modem auto-recovery enable command to enable forced auto recovery.<br>Use the undo modem auto-recovery enable command to restore the default.<br>By default, forced auto recovery is disabled.<br>With this function enabled, if the dialup fails continuously for multiple times, the system automatically resets the modem.<br>With this function disabled, the system automatically resets the modem only when the 3G modem has a successful dialup record after the last modem reset and the 3G modem fails to dial up continuously for multiple times.<br>To set the dialup failure times after which the 3G modem is reset, use the auto-recovery keyword in the modem response command.<br>This function avoids the failures to restore links caused by an abnormal 3G network.<br>When you enable this function, make sure that the other configurations are correct. Incorrect configurations may reset the modem.<br>Related commands: modem response.<br>Examples<br># Enable forced auto recovery for interface Cellular 1/0.<br><Sysname> system-view<br>[Sysname]interface cellular 1/0<br>[Sysname-Cellular0/0] modem auto-recovery enable<br>4. Syntax<br>**mirror number** *number* { **pcm** \| { **in** \| **out** \| **all** } { **command** \| **data** } } **to** { **local-interface** *interface-type interface-number* [ **mac** H-H-H ] \| **remote-ip** *ip-address* [ **port** *port* ] }<br>**undo mirror** [**number** *number*]<br>View<br>Analog subscriber line view<br>Parameters<br>number *number*: Mirror entry number, in the range of 1 to 64.<br>pcm: Mirrors PCM data.<br>in: Mirrors inbound RTP or command data.<br>out: Mirrors outbound RTP or command data.<br>all: Mirrors bidirectional RTP or command data.<br>data: Mirrors RTP data.<br>command: Mirrors command data.<br>to: Specifies an output interface or destination IP address for mirrored traffic.<br>local-interface *interface-type interface-number*: Specifies an output interface, which must be a Layer-2 or Layer-3 Ethernet port.<br>mac: Specifies the destination MAC address for mirrored traffic, in the format H-H-H. You can remove the leading 0s in Hs from the MAC address. For example, f-e2-1 represents 000f-00e2-0001.<br>remote-ip *ip-address*: Specifies the destination IP address<br>port *port*: Specifies a destination port for mirrored traffic. The default port is |

| Item | Description |
| --- | --- |
| | 60000.<br>Description<br>Use the mirror command to mirror the PCM, RTP, or voice command data on the subscriber line to a specified interface or destination.<br>Use the undo mirror command to remove a mirror entry or all mirror entries.<br>By default, no traffic is mirrored.<br>The router allows only one PCM data mirror entry to exist.<br>This command is only applicable to FXS, FXO, and E&M analog subscriber lines.<br>Examples<br># Mirror PCM data on the interface FXS 1/0 to the interface Ethernet1/1.<br><Sysname> system-view<br>[Sysname] subscriber-line 1/0<br>[Sysname-subscriber-line1/0] mirror number 1 pcm to local-interface ethernet 1/1<br>5. Syntax<br>To mirror PCM or RTP data based on a calling number, use the command:<br>**mirror number** *number* { **pcm** \| { **in** \| **out** \| **all** } **data** } **calling** *calling-number* **to** { **local-interface** *interface-type interface-number* [ **mac** H-H-H ] \| **remote-ip** *ip-address* [ **port** *port* ] }<br>**undo mirror** [**number** *number*]<br>To mirror PCM data based on a time slot, use the command:<br>**mirror number** *number* **pcm** { **bdsp** \| **fdsp** } *channel-number* **to** { **local-interface** *interface-type interface-number* [ **mac** H-H-H ] \| **remote-ip** *ip-address* [ **port** *port* ] }<br>**undo mirror** [**number** *number*]<br>To mirror RTP or command data on all time slots, use the command:<br>**mirror number** *number* { **in** \| **out** \| **all** } { **command** \| **data** } **to** { **local-interface** *interface-type interface-number* [ **mac** H-H-H ] \| **remote-ip** *ip-address* [ **port** *port* ] }<br>**undo mirror** [**number** *number*]<br>View<br>Digital subscriber line view<br>Parameters<br>number *number*: Mirror entry number, in the range of 1 to 64.<br>pcm: Mirrors PCM data.<br>in: Mirrors inbound RTP or command data.<br>out: Mirrors outbound RTP or command data.<br>all: Mirrors bidirectional RTP or command data.<br>data: Mirrors RTP data.<br>command: Mirrors command data.<br>calling *calling-number*: Specifies a calling number, a string of up to 31 characters that can only contain 0 through 9. Traffic matching the specified calling number will be mirrored.<br>bdsp: Mirrors the PCM data of the back-end DSP of the specified time slot.<br>fdsp: Mirrors the PCM data of front-end DSP of the specified time slot. |

| Item | Description |
|---|---|
| | command: Mirrors command data.<br>*channel-number*: Specifies a time slot in the range of 0 to 29. The data on the specified time slot will be mirrored.<br>to: Specifies an output interface or destination IP address for mirrored traffic.<br>local-interface *interface-type interface-number*: Specifies an output interface, which must be a Layer-2 or Layer-3 Ethernet port.<br>mac: Specifies the destination MAC address for mirrored traffic, in the format H-H-H. You can remove the leading 0s in Hs from the MAC address. For example, f-e2-1 represents 000f-00e2-0001.<br>remote-ip *ip-address*: Specifies the destination IP address for mirrored traffic.<br>port *port*: Specifies a destination port for mirrored traffic. The default port is 60000.<br>Description<br>Use the mirror command to mirror the data of a calling number to a specified interface or destination.<br>Use the undo mirror command to remove a mirror entry or all mirror entries.<br>By default, no traffic is mirrored.<br>The router allows only one PCM data mirror entry to exist.<br>This command is only applicable to the digital subscriber lines generated on VE1, VT1, and BSV interfaces.<br>Examples<br># Mirror the PCM data of the calling number 55501234 to the interface Ethernet1/1 on subscriber-line 1/0:0 generated on the VE1 interface.<br><Sysname> system-view<br>[Sysname] subscriber-line 1/0:0<br>[Sysname-subscriber-line1/0:0] mirror number 1 pcm calling 55501234 to local-interface ethernet 1/1<br>6. Syntax<br>**e1pos-adaptor**<br>**undo e1pos-adaptor**<br>Views<br>System view<br>Parameters<br>None<br>Description<br>Use the e1pos-adaptor command to create the E1POS interface maintenance service and enter its view.<br>Use the undo e1pos-adaptor command to delete the E1POS interface maintenance service.<br>By default, no E1POS interface maintenance service is configured.<br>Examples<br># Create the E1POS interface maintenance service and enter its view.<br><Sysname> system-view<br>[Sysname] e1pos-adaptor |

| Item | Description |
| --- | --- |
| | [Sysname-e1pos-adaptor]<br>7. Syntax<br>**parameter enable**<br>**undo parameter enable**<br>Views<br>E1POS interface maintenance service view<br>Parameters<br>None<br>Description<br>Use the parameter enable command to enable negotiation parameter selection as per calling number.<br>Use the undo parameter enable command to disable negotiation parameter selection as per calling number.<br>By default, negotiation parameter selection as per calling number is enabled.<br>Examples<br># Enable negotiation parameter selection as per calling number.<br><Sysname> system-view<br>[Sysname] e1pos-adaptor<br>[Sysname-e1pos-adaptor] parameter enable<br>8. Syntax<br>**parameter-group** *group-number*<br>**undo parameter-group** { *group-number* \| **all** }<br>Views<br>E1POS interface maintenance service view<br>Parameters<br>*group-number*: Calling number negotiation parameter group number, which ranges from 1 to 128.<br>Description<br>Use the parameter-group command to create a calling number negotiation parameter group and enter its view.<br>Use the undo parameter-group command to delete the specified or all calling number negotiation parameter groups.<br>By default, no calling number negotiation parameter group is configured.<br>In calling number negotiation parameter view, you can use the negotiation and threshold commands to configure negotiation parameters.<br>Examples<br># Create calling number negotiation parameter group 1 and enter its view.<br><Sysname> system-view<br>[Sysname] e1pos-adaptor<br>[Sysname-e1pos-adaptor] parameter-group 1<br>9. Syntax<br>**calling-number** *calling-number* **apply** *group-number* |

| Item | Description |
| --- | --- |
| | **undo calling-number** { *calling-number* \| **all** }<br>Views<br>E1POS interface maintenance service view<br>Parameters<br>*calling-number*: Calling number matching a negotiation parameter group. The calling number is a string of up to 31 characters, which can be 0 to 9, period (.), and T.<br>0 to 9 represent the numbers between 0 and 9. One number is a digit.<br>A period (.) is a wildcard and can match one effective digit. For example, *555. . . .* matches any number string that starts with 555 and has four digits followed.<br>T indicates the timer, and means that the user can dial any number until the number is too long, the number end is dialed, or the timer expires. T is used to match a number which is of any length and starts with the string before T. For example, 555T matches any number string that starts with 555.<br>*group-number*: Calling number negotiation parameter group number, which ranges from 1 to 128.<br>Description<br>Use the calling-number command to specify a negotiation parameter group to match a calling number.<br>Use the undo calling-number command to delete the specified or all calling numbers.<br>You can specify a negotiation parameter group to match up to 512 calling numbers.<br>By default, no negotiation parameter group is specified to match a calling number.<br>In negotiation parameter group view, you can use the negotiation and threshold commands to configure negotiation parameters.<br>Examples<br># Configure negotiation parameter group 1 to match the calling numbers starting with 555.<br><Sysname> system-view<br>[Sysname] e1pos-adaptor<br>[Sysname-e1pos-adaptor] calling-number 555T apply 1<br>10. Syntax<br>**mirror number** *number* **pcm calling** *calling-number* **to** { **local-interface** *interface-type interface-number* [ **mac** H-H-H ] \| **remote-ip** *ip-address* [ **port** *port* ] }<br>**undo mirror** [ **number** *number* ]<br>Views<br>E1POS interface maintenance service view<br>Default level<br>2: System level<br>Parameters<br>number *number*: Specifies a mirror entry number, which ranges from 1 to 64.<br>pcm: Mirrors the PCM data. |

| Item | Description |
| --- | --- |
| | calling *calling-number*: Specifies the calling number whose PCM data is to be mirrored. The calling number must be exactly matched, and is a string of up to 31 characters, which must be numbers 0 through 9.<br>to: Mirrors the packets to the specified interface or IP address.<br>local-interface *interface-type interface-number*: Mirrors the PCM data of the specified calling number to an interface specified its type and number. The interface must be a Layer 2 or Layer 3 Ethernet interface.<br>mac: Specifies the destination MAC address of the mirrored packets.<br>remote-ip *ip-address*: Mirrors the PCM data of the specified calling number to the specified IP address.<br>port *port*: Mirrors the PCM data to the specified port number, which is 60000 by default.<br>Description<br>Use the mirror command to mirror the PCM data of the specified calling number.<br>Use the undo mirror command to delete the specified or all mirror entries.<br>By default, no data is mirrored.<br>Only one PCM data mirror entry can exist on a router.<br>Examples<br># Mirror the PCM data of calling number 55501234 to interface Ethernet 1/1.<br><Sysname> system-view<br>[Sysname] e1pos-adaptor<br>[Sysname-e1pos-adaptor] mirror number 1 pcm calling 55501234 to local-interface ethernet 1/1<br>11. Syntax<br>**mirror number** *number* **pcm** *channel-number* **to** { **local-interface** *interface-type interface-number* [ **mac** H-H-H ] \| **remote-ip** *ip-address* [ **port** *port* ] }<br>**undo mirror** [ **number** *number* ]<br>Views<br>FCM interface view<br>Parameters<br>number *number*: Specifies a mirror entry number, which ranges from 1 to 64.<br>pcm: Mirrors the PCM data.<br>*channel-number*: Number of the E1POS interface channel whose PCM data is to be mirrored. This argument ranges from 0 to 29.<br>to: Mirrors the packets to the specified interface or IP address.<br>local-interface *interface-type interface-number*: Mirrors the PCM data of the specified E1POS interface channel to an interface specified its type and number. The interface must be a Layer 2 or Layer 3 Ethernet interface.<br>mac: Specifies the destination MAC address (in the format of H-H-H-H) of the mirrored packets. When inputting an MAC address, you can omit the starting zeros in each section. For example, you can simply input f-e2-1 for 000f-00e2-0001.<br>remote-ip *ip-address*: Mirrors the PCM data of the specified E1POS interface channel to the specified IP address. |

| Item | Description |
| --- | --- |
| | port *port*: Mirrors the PCM data to the specified port number, which is 60000 by default.<br>Description<br>Use the mirror command to mirror the PCM data of the specified E1POS interface channel.<br>Use the undo mirror command to delete the specified or all mirror entries.<br>By default, no data is mirrored.<br>Only one PCM data mirror entry can exist on a router.<br>Examples<br># Mirror the PCM data of channel 2 on interface FCM 1/0:15 to interface Ethernet 1/1.<br><Sysname> system-view<br>[Sysname] interface fcm 1/0:15<br>[Sysname-fcm1/0:15] mirror number 1 pcm 2 to local-interface ethernet 1/1<br>12. Syntax<br>**display logfile status**<br>View<br>Any view<br>Parameters<br>None<br>Description<br>Use the display logfile status command to display the state of output of system information to the log file function on MSR 20-1X.<br>This command only supported on MSR 20-1X routers.<br>Examples<br># Display the state of output of system information to the log file function.<br><Sysname> display logfile status<br>Current Log File Status: disable<br>Next reboot Log File Status: enable<br>13. Syntax<br>**logfile { enable \| disable }**<br>View<br>Any view<br>Parameters<br>**enable**: Enable the output of system information to the log file.<br>**disable**: Disable the output of system information to the log file.<br>Description<br>Use the logfile enable command to enable the output of system information to the log file on MSR 20-1X.<br>Use the logfile disable command to disable the output of system information to the log file on MSR 20-1X.<br>Enable or disable this feature, you need to restart the router to take effect.<br>By default, output of system information to the log file is enabled.<br>This command only supported on MSR 20-1X routers. |

| Item | Description |
| --- | --- |
| | Examples<br># Enable the output of system information to the log file on MSR 20-1X.<br><Sysname> logfile enable |
| Removed commands | None |
| Modified commands | 1.<br>Original command: **sendat** *at-string*<br>Modified command: **sendat** *at-string*<br>Module of the command: Modem management command<br>Description: *at-string*: Add the value ranges: A string of 1 to 256 characters.<br>Changes in default values: None.<br>Changes in value ranges: *at-string*: Add the value ranges: A string of 1 to 256 characters.<br>2.<br>Original command:<br>**key** { **accounting** \| **authentication** \| **authorization** } *key*<br>**undo key** { **accounting** \| **authentication** \| **authorization** }<br>Modified command:<br>**key** { **accounting** \| **authentication** \| **authorization** } *key*<br>**undo key** { **accounting** \| **authentication** \| **authorization** }<br>Module of the command: AAA<br>Description: *key*: Shared key, a case-sensitive string whose value range changes from 1~64 characters to 1~255 characters.<br>Changes in default values: None.<br>Changes in value ranges: *key*: Shared key, a case-sensitive string whose value range changes from 1~64 characters to 1~255 characters. |
| CMW520-R2207P02 | |
| New commands | 1. Syntax<br>**eoapad enable**<br>**undo eoapad enable**<br>View<br>ATM interface view<br>Parameters<br>None<br>Description<br>Use the eoapad enable command to enable padding for Ethernet packets smaller than 60 bytes.<br>Use the undo eoa pad enable command to restore the default.<br>By default, the padding for Ethernet packets smaller than 60 bytes is disabled.<br>This command enables the PVC to pad Ethernet packets smaller than 60 bytes on the PVC to prevent the packets from being discarded.<br>Examples |

| Item | Description |
| --- | --- |
| | # Enable padding for Ethernet packets on interface ATM 1/0/1.<br><Sysname> system-view<br>[Sysname] interface atm 1/0/1<br>[Sysname-Atm1/0/1] eoapad enable |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2207 | |
| New commands | 1.<br>**address** *index-number* { **ipv4** *ip-address* \| **dns** *dns-name* } [ **port** *port-number* ] [ **transport** { **udp** \| **tcp** \| **tls** } ] [ **url** { **sip** \| **sips** } ]<br>**undo address** *index-number*<br>2.<br>**address sip server-group** *group-number*<br>**undo address sip server-group**<br>3.<br>**assign { host-name** *host-name* \| **contact-user** *user-name* **}**<br>**undo assign { host-name \| contact-user }**<br>4.<br>**account enable**<br>**undo account enable**<br>5.<br>**bind sip-trunk account** *account-index*<br>**undo bind sip-trunk account**<br>6.<br>**description** *text*<br>**undo description**<br>7.<br>**display voice sip-trunk account**<br>8.<br>**display voice server-group** [ *group-number* ]<br>9.<br>**group-name** *group-name*<br>**undo group-name**<br>10.<br>**hot-swap enable**<br>**undo hot-swap enable**<br>11.<br>**keepalive { options [ interval** ***seconds*** **] \| register }**<br>**undo keepalive**<br>12.<br>**match source host-prefix** *host-prefix*<br>**undo match source host-prefix** |

| Item | Description |
| --- | --- |
| | 13.<br>**match destination host-prefix** *host-prefix*<br>**undo match destination host-prefix**<br>14.<br>**match source address { ipv4** ***ip-address*** **\| dns** ***dns-name*** **\| server-group** ***group-number*** **}**<br>**undo match source address**<br>15.<br>**proxy server-group** *group-number*<br>**undo proxy server-group**<br>16.<br>**registrar server-group** *group-number* **[ expires** ***seconds*** **]**<br>**undo registrar server-group**<br>17.<br>**register enable**<br>**undo register enable**<br>18.<br>**redundancy mode { parking \| homing }**<br>**undo redundancy mode**<br>19.<br>**server-group** *group-number*<br>**undo server-group** { *group-number* \| **all** }<br>20.<br>**sip-trunk account** *account-index*<br>**undo sip-trunk account** { *account-index* \| **all** }<br>21.<br>**sip-trunk enable**<br>**undo sip-trunk enable**<br>22.<br>**timer registration retry** *seconds*<br>**undo timer registration retry**<br>23.<br>**timer registration expires** *seconds*<br>**undo timer registration expires**<br>24.<br>**timer registration divider** *percentage*<br>**undo timer registration divider**<br>25.<br>**timer registration threshold** *seconds*<br>**undo timer registration threshold**<br>26.<br>**user** *username* **password { cipher \| simple }** *password*<br>**undo user** |

| Item | Description |
| --- | --- |
| | 27.<br>**media-protocol { rtp** \| **srtp } ***<br>**undo media-protocol**<br>28.<br>**display ve-group** [ *ve-group-id* ] [ **slot** *slot-number* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>29.<br>**ve-group** ***ve-group-id*** **{ terminate** \| **access }**<br>**undo ve-group**<br>30.<br>**early-media enable**<br>**undo early-media enable**<br>31.<br>**reverse-route tag** *tag-value*<br>**undo reverse-route tag**<br>32.<br>**reverse-route preference** *preference-value*<br>**undo reverse-route preference**<br>33.<br>**reverse-route [ remote-peer** *ip-address* **[ gateway** \| **static ]** \| **static ]**<br>**undo reverse-route**<br>34.<br>**display bgp vpnv6 all peer [** *ipv4-address* **verbose** \| **verbose ] [** \| **{ begin** \| **exclude** \| **include }** *regular-expression* **]**<br>35.<br>**display bgp vpnv6 all routing-table** [ *network-address prefix-length* [ **longer-prefixes** ] \| **peer** *ip-address* { **advertised-routes** \| **received-routes } [ statistic ]** \| **statistic ] [** \| **{ begin** \| **exclude** \| **include** } *regular-expression* ]<br>36.<br>**display bgp vpnv6 route-distinguisher** *route-distinguisher* **routing-table** [ *network-address prefix-length* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>37.<br>**display bgp vpnv6 vpn-instance** *vpn-instance-name* **peer** [ *ipv6-address* verbose \| verbose ] [ \| { begin \| exclude \| include } *regular-expression* ]<br>38.<br>**display bgp vpnv6 vpn-instance** *vpn-instance-name* **routing-table** [ *network-address prefix-length* [ **longer-prefixes** ] \| **peer** *ipv6-address* { **advertised-routes** \| **received-routes** } ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>39.<br>**display ipv6 fib vpn-instance** *vpn-instance-name* [ **acl6** *acl6-number* \| **ipv6-prefix** *ipv6-prefix-name* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>40.<br>**display ipv6 fib vpn-instance** *vpn-instance-name ipv6-address* |

| Item | Description |
| --- | --- |
| | [ *prefix-length* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>41.<br>**filter-policy** { *acl6-number* \| **ipv6-prefix** *ipv6-prefix-name* } **export** [ **direct** \| **isisv6** *process-id* \| **ospfv3** *process-id* \| **ripng** *process-id* \| **static** ]<br>**undo filter-policy export** [ **direct** \| **isisv6** *process-id* \| **ospfv3** *process-id* \| **ripng** *process-id* \| **static** ]<br>42.<br>**filter-policy** { *acl6-number* \| **ipv6-prefix** *ipv6-prefix-name* } **import**<br>**undo filter-policy import**<br>43.<br>**ipv4-family (VPN instance view)**<br>**undo ipv4-family (VPN instance view)**<br>44.<br>**ipv6-family { vpnv6** \| **vpn-instance** *vpn-instance-name* } **(BGP view)**<br>**undo ipv6-family { vpnv6** \| **vpn-instance** *vpn-instance-name* } **(BGP view)**<br>45.<br>**ipv6-family (VPN instance view)**<br>**undo ipv6-family (VPN instance view)**<br>46.<br>**peer** *ip-address* **enable** (BGP-VPNv6 subaddress family view)<br>**undo peer** *ip-address* **enable**(BGP-VPNv6 subaddress family view)<br>47.<br>**peer** *ip-address* **filter-policy** *acl6-number* { **export** \| **import** } (BGP-VPNv6 subaddress family view)<br>**undo peer** *ip-address* **filter-policy** [ *acl6-number* ] { **export** \| **import** } (BGP-VPNv6 subaddress family view)<br>48.<br>**peer** *ip-address* **ipv6-prefix** *prefix-name* **{ export** \| **import }**<br>**undo peer** *ip-address* **ipv6-prefix { export** \| **import }**<br>49.<br>**peer** *ip-address* **preferred-value** *value* (BGP-VPNv6 subaddress family view)<br>**undo peer** *ip-address* **preferred-value**(BGP-VPNv6 subaddress family view)<br>50.<br>**peer** *ip-address* **public-as-only** (BGP-VPNv6 subaddress family view)<br>**undo peer** *ip-address* **public-as-only** (BGP-VPNv6 subaddress family view)<br>51.<br>**peer** *ip-address* **reflect-client** (BGP-VPNv6 subaddress family view)<br>**undo peer** *ip-address* **reflect-client** (BGP-VPNv6 subaddress family view)<br>52.<br>**peer** *ip-address* **route-policy** *route-policy-name* { **export** \| **import** } (BGP-VPNv6 subaddress family view)<br>**undo peer** *ip-address* **route-policy** *route-policy-name* { **export** \| **import** } (BGP-VPNv6 subaddress family view) |

| Item | Description |
| --- | --- |
| | 53.<br>**refresh bgp ipv6 vpn-instance** *vpn-instance-name* { *ipv6-address* \| **all** \| **external** } { **export** \| **import** }<br>54.<br>**refresh bgp vpnv6** { *ip-address* \| **all** \| **external** \| **internal** } { **export** \| **import** }<br>55.<br>**reset bgp ipv6 vpn-instance** *vpn-instance-name* { *as-number* \| *ipv6-address* \| **all** \| **external** }<br>56.<br>**reset bgp vpnv6** { *as-number* \| *ip-address* \| **all** \| **external** \| **internal** }<br>57.<br>**display multicast [ all-instance** \| **vpn-instance** *vpn-instance-name* ] **forwarding-table df-info** [ *rp-address* ] [ \| **{ begin** \| **exclude** \| **include }** *regular-expression* ]<br>58.<br>**display multicast ipv6 forwarding-table df-info** [ *rp-address* ] [ \| **{ begin** \| **exclude** \| **include** } *regular-expression*<br>59.<br>**bidir-pim enable**<br>**undo bidir-pim enable**<br>60.<br>**display pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] **df-info** [ *rp-address* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>61.<br>**bidir-pim enable**<br>**undo bidir-pim enable**<br>62.<br>**display pim ipv6 df-info** [ *rp-address* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>63.<br>**isdn progress-indicator** *indicator*<br>**undo isdn progress-indicator** [ *indicator* ]<br>64.<br>**outbound-proxy** { **dns** *domain-name* \| **ipv4** *ip-address* } [ **port** *port-number* ]<br>**undo outbound-proxy { dns** \| **ipv4 }**<br>65.<br>**uri user-info user-info** [ **domain** *domain-name* ]<br>**undo uri**<br><br>Refer to About the HP A-MSR Command References. |
| Removed commands | None |
| Modified commands | 1. |

| Item | Description |
| --- | --- |
| | Original command:<br>**mpls l2vc** *destination vcid* **[ tunnel-policy** *tunnel-policy-name* **]** **[ control-word** \| **no-control-word ]**<br>**undo mpls l2vc**<br>Modified command:<br>**mpls l2vc** *destination vcid* **[ { control-word** \| **ethernet** \| **ip-interworking** \| **no-control-word** \| **vlan } \|** **[ tunnel-policy** *tunnel-policy-name* **]** **[ backup-peer** *ip-address vcid* **[ backup-tunnel-policy** *tunnel-policy-name* \| **revertive [ wtr-time** *wtr-time* **] ] * ] ] ***<br>**undo mpls l2vc**<br>Module of the command: MPLS<br>Description: Change this command from **[ tunnel-policy** *tunnel-policy-name* **] [ control-word** \| **no-control-word ]** to **[ { control-word** \| **ethernet** \| **ip-interworking** \| **no-control-word** \| **vlan } \|** **[ tunnel-policy** *tunnel-policy-name* **] [ backup-peer** *ip-address vcid* **[ backup-tunnel-policy** *tunnel-policy-name* \| **revertive [ wtr-time** *wtr-time* **] ] * ] ] *.**<br>Use the mpls l2vc command to create a Martini L2VPN connection.<br>Use the undo mpls l2vc command to delete the Martini connection on the CE interface.<br>If you do not specify the tunneling policy, or if you specify the tunneling policy name but do not configure the policy, the default policy is used for the VC. The default tunneling policy selects only one tunnel in this order: LSP tunnel, GRE tunnel, CR-LSP tunnel.<br>Only L2VPNs that use ATM, PPP, FR, or HDLC encapsulation support the control word option.<br>The PW encapsulation type can be Ethernet or VLAN. The device allows you to specify the PW encapsulation type for only Layer 3 Ethernet interfaces and subinterfaces, Layer 3 virtual Ethernet interfaces and subinterfaces, and VLAN interfaces. When not specified, the PW encapsulation type depends on the interface type: it is Ethernet on Layer 3 Ethernet interfaces and Layer 3 virtual Ethernet interfaces, and VLAN on Layer 3 Ethernet subinterfaces, Layer 3 virtual Ethernet subinterfaces, and VLAN interfaces.<br>Parameters:<br>destination: IP address of the peer PE.<br>vc-id: VC ID of the L2VPN connection, in the range 1 to 4294967295.<br>control-word: Enables the control word option. Support for this keyword depends on the device model.<br>no-control-word: Disables the control word option. Support for this keyword depends on the device model.<br>ethernet: Specifies the PW encapsulation type of Ethernet. In Ethernet mode, P-Tag is not transferred on the PW. If a packet from a CE contains the service delimiter, the PE removes the service delimiter and adds a PW label and tunnel label into the packet before sending the packet out. If a packet from a CE contains no delimiter, the PE directly adds a PW label and a tunnel label into the packet and then sends the packet out. For a packet to be sent downstream, you can configure the PE to add or not add the service delimiter into the packet, but rewriting and removing of existing tags are not allowed. Support for this keyword depends on the device model.<br>ip-interworking: Enables support for the MPLS L2VPN interworking feature. |

| Item | Description |
| --- | --- |
| | Support for this keyword depends on the device model.<br>vlan: Specifies the PW encapsulation type of VLAN. In VLAN mode, packets transmitted over the PW must carry a P-Tag. For a packet from a CE, if it contains the service delimiter, the PE keeps the P-TAG unchanged or changes the P-tag to the VLAN tag expected by the peer PE or to a null tag (the tag value is 0), and then adds a PW label and a tunnel label into the packet before sending the packet out. If the packet contains no service delimiter, the PE adds the VLAN tag expected by the peer PE or a null tag, and then a PW label and a tunnel label into the packet before sending the packet out. For a packet to be sent downstream, the PE rewrites, removes, or retains the service delimiter depending on your configuration. Support for this keyword depends on the device model.<br>tunnel-policy tunnel-policy-name: Specifies the tunneling policy for the VC. The tunneling policy name is a case insensitive string of 1 to 19 characters.<br>backup-peer ip-address vcid: Specifies the IP address of the backup link's peer PE and the VC ID of the backup link. The VC ID ranges from 1 to 4294967295. Support for this keyword and argument combination depends on the device model.<br>backup-tunnel-policy tunnel-policy-name: Specifies the tunneling policy for the backup link. The tunneling policy name is a case insensitive string of 1 to 19 characters. Support for this keyword and argument combination depends on the device model.<br>revertive: Enables support for switchback. With this keyword specified, when the main link recovers, traffic is switched from the backup link back to the main link automatically. Traffic will not be switched back automatically if you do not specify this keyword. Support for this keyword depends on the device model.<br>wtr-time wtr-time: Specifies switchback delay time. After the main link recovers, the device waits for a period of time dictated by the switchback delay time before switching the traffic from the backup link back to the main link. The wtr-time argument ranges from 1 to 720 and defaults to 30, in minutes. Support for this keyword and argument combination depends on the device model.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.<br>Original command:<br>**mpls static-l2vc destination** *destination-router-id* **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* **[ tunnel-policy** *tunnel-policy-name* **] [ control-word** \| **no-control-word ]**<br>**undo mpls static-l2vc**<br>Modified command:<br>**mpls static-l2vc destination** *destination-router-id* **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* **[ { control-word** \| **ethernet** \| **ip-interworking** \| **no-control-word** \| **vlan } \|** **tunnel-policy** *tunnel-policy-name* **] ***<br>**undo mpls static-l2vc**<br>Module of the command: MPLS<br>Description: Change this command from **[ tunnel-policy** *tunnel-policy-name* **] [ control-word** \| **no-control-word ]** to **[ { control-word** \| **ethernet** \| **ip-interworking** \| **no-control-word** \| **vlan }** \| **tunnel-policy** |

| Item | Description |
| --- | --- |
| | *tunnel-policy-name* **] ***.<br><br>Use the mpls static-l2vc command to create a static VC between CEs connected to different PEs.<br><br>Use the undo mpls static-l2vc command to delete the static VC.<br><br>You must configure the command on both PEs. The destination address is the IP address of the peer PE. The outgoing label and incoming label are, respectively, the incoming label and outgoing label of the peer.<br><br>If you do not specify the tunneling policy, or if you specify the tunneling policy name but do not configure the policy, the default policy is used for the VC. The default tunneling policy selects only one tunnel in this order: LSP tunnel, GRE tunnel, CR-LSP tunnel.<br><br>Only L2VPNs using ATM, PPP, FR, or HDLC encapsulation supports the control word option.<br><br>The PW encapsulation type can be Ethernet or VLAN. The device allows you to specify the PW encapsulation type for only Layer 3 Ethernet interfaces and subinterfaces, Layer 3 virtual Ethernet interfaces and subinterfaces, and VLAN interfaces. When not specified, the PW encapsulation type depends on the interface type: it is Ethernet on Layer 3 Ethernet interfaces and Layer 3 virtual Ethernet interfaces, and VLAN on Layer 3 Ethernet subinterfaces, Layer 3 virtual Ethernet subinterfaces, and VLAN interfaces.<br><br>Parameters:<br><br>destination dest-router-id: Specifies a destination router ID.<br><br>transmit-vpn-label transmit-label-value: Specifies an outgoing label for the VPN, or, the outgoing label for the static level 2 VC. The value ranges from 16 to 1023.<br><br>receive-vpn-label receive-label-value: Specifies an incoming label for the VPN, or, the incoming label for the static level 2 VC. The value ranges from 16 to 1023.<br><br>control-word: Enables the control word option. Support for this keyword depends on the device model.<br><br>ethernet: Specifies the PW encapsulation type of Ethernet. In Ethernet mode, P-Tag is not transferred on the PW. If a packet from a CE contains the service delimiter, the PE removes the service delimiter and adds a PW label and tunnel label into the packet before sending the packet out. If a packet from a CE contains no delimiter, the PE directly adds a PW label and a tunnel label into the packet and then sends the packet out. For a packet to be sent downstream, you can configure the PE to add or not add the service delimiter into the packet, but rewriting and removing of existing tags are not allowed. Support for this keyword depends on the device model.<br><br>ip-interworking: Enables support for the MPLS L2VPN interworking feature. Support for this keyword depends on the device model.<br><br>no-control-word: Disables the control word option. Support for this keyword depends on the device model.<br><br>vlan: Specifies the PW encapsulation type of VLAN. In VLAN mode, packets transmitted over the PW must carry a P-Tag. For a packet from a CE, if it contains the service delimiter, the PE keeps the P-TAG unchanged or changes the P-tag to the VLAN tag expected by the peer PE or to a null tag (the tag value is 0), and then adds a PW label and a tunnel label into the packet before sending the packet out. If the packet contains no service delimiter, the PE adds the VLAN tag expected by the peer PE or a null tag, and then a PW label and a tunnel label into the packet before |

| Item | Description |
|---|---|
| | sending the packet out. For a packet to be sent downstream, the PE rewrites, removes, or retains the service delimiter depending on your configuration. Support for this keyword depends on the device model.<br>tunnel-policy tunnel-policy-name: Specifies an tunneling policy for the VC, a string of 1 to 19 characters.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>3.<br>Original command:<br>**static-rp** *rp-address* [ *acl-number* ] **[ preferred ]**<br>Modified command:<br>**static-rp** *rp-address* [ *acl-number* ] [ **preferred** ] [ **bidir** ]<br>Module of the command: PIM<br>Description: Add a new parameter of **bidir**.<br>bidir: Configures the static RP to serve multicast groups in BIDIR-PIM. Without this argument, the static RP serves groups in PIM-SM.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>4.<br>Original command:<br>**debugging pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] { **all** \| **assert** [ *advanced-acl-number* ] [ **receive** \| **send** ] \| **event** [ *advanced-acl-number* ] \| **join-prune** [ *advanced-acl-number* ] [ **receive** \| **send** ] \| **msdp** [ *advanced-acl-number* ] \| **neighbor** [ *basic-acl-number* ] [ **receive** \| **send** ] \| **register** [ *advanced-acl-number* ] \| **routing-table** [ *advanced-acl-number* ] \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ *advanced-acl-number* ] [ **receive** \| **send** ] }<br>**undo debugging pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] { **all** \| **assert** [ **receive** \| **send** ] \| **event** \| **join-prune** [ **receive** \| **send** ] \| **msdp** \| **neighbor** [ **receive** \| **send** ] \| **register** \| **routing-table** \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ **receive** \| **send** ] }<br>Modified command:<br>**debugging pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] { **all** \| **assert** [ *advanced-acl-number* ] [ **receive** \| **send** ] \| **df** \| **event** [ *advanced-acl-number* ] \| **join-prune** [ *advanced-acl-number* ] [ **receive** \| **send** ] \| **msdp** [ *advanced-acl-number* ] \| **neighbor** [ *basic-acl-number* ] [ **receive** \| **send** ] \| **register** [ *advanced-acl-number* ] \| **routing-table** [ *advanced-acl-number* ] \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ *advanced-acl-number* ] [ **receive** \| **send** ] }<br>**undo debugging pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] { **all** \| **assert** [ **receive** \| **send** ] \| **df** \| **event** \| **join-prune** [ **receive** \| **send** ] \| **msdp** \| **neighbor** [ **receive** \| **send** ] \| **register** \| **routing-table** \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ **receive** \| **send** ] }<br>Module of the command: PIM<br>Description: Add a new parameter of **df**.<br>df: Debugging for DF information of PIM.<br>Changes in default values: None.<br>Changes in value ranges: None. |

| Item | Description |
| --- | --- |
| | 5.<br>Original command:<br>**static-rp** *ipv6-rp-address* [ *acl6-number* ] [ **preferred** ]<br>Modified command:<br>**static-rp** *ipv6-rp-address* [ *acl6-number* ] [ **preferred** ] [ **bidir** ]<br>Module of the command: PIM<br>Description: Add a new parameter of **bidir**.<br>bidir: Configures the static RP to serve multicast groups in IPv6 BIDIR-PIM. Without this argument, the static RP serves groups in IPv6 PIM-SM.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>6.<br>Original command:<br>**debugging pim ipv6** { **all** \| **assert** [ *advanced-acl6-number* ] [ **receive** \| **send** ] \| **event** [ *advanced-acl6-number* ] \| **join-prune** [ *advanced-acl6-number* ] [ **receive** \| **send** ] \| **neighbor** [ *basic-acl6-number* ] [ **receive** \| **send** ] \| **register** [ *advanced-acl6-number* ] \| **routing-table** [ *advanced-acl6-number* ] \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ *advanced-acl6-number* ] [ **receive** \| **send** ] }<br>**undo debugging pim ipv6** { **all** \| **assert** [ **receive** \| **send** ] \| **event** \| **join-prune** [ **receive** \| **send** ] \| **neighbor** [ **receive** \| **send** ] \| **register** \| **routing-table** \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ **receive** \| **send** ] }<br>Modified command:<br>**debugging pim ipv6** { **all** \| **assert** [ *advanced-acl6-number* ] [ **receive** \| **send** ] \| **df** \| **event** [ *advanced-acl6-number* ] \| **join-prune** [ *advanced-acl6-number* ] [ **receive** \| **send** ] \| **neighbor** [ *basic-acl6-number* ] [ **receive** \| **send** ] \| **register** [ *advanced-acl6-number* ] \| **routing-table** [ *advanced-acl6-number* ] \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ *advanced-acl6-number* ] [ **receive** \| **send** ] }<br>**undo debugging pim ipv6** { **all** \| **assert** [ **receive** \| **send** ] \| **df** \| **event** \| **join-prune** [ **receive** \| **send** ] \| **neighbor** [ **receive** \| **send** ] \| **register** \| **routing-table** \| **rp** [ **receive** \| **send** ] \| **state-refresh** [ **receive** \| **send** ] }<br>Module of the command: PIM<br>Description: Add a new parameter of **df**.<br>df: Debugging for DF information of IPv6 PIM.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>7.<br>Original command:<br>**defense icmp-flood ip** *ip-address* **[ max-rate** *rate-number* **]**<br>**undo defense icmp-flood ip** *ip-address* **[ max-rate ]**<br>Modified command:<br>**defense icmp-flood ip** *ip-address* **rate-threshold high** *rate-number* **[ low** *rate-number* **]**<br>**undo defense icmp-flood ip** *ip-address* **[ rate-threshold ]**<br>Module of the command: Security |

| Item | Description |
| --- | --- |
| | Description: Change the parameter of **defense icmp-flood ip** from **[ max-rate** *rate-number* **]** to **rate-threshold high** *rate-number* **[ low** *rate-number* **]**. And change the command of **undo defense icmp-flood ip** from **[ max-rate ]** to **[ rate-threshold ].**<br>Parameters:<br>high rate-number: Sets the action threshold for ICMP flood attack protection of the specified IP address. rate-number indicates the number of ICMP packets sent to the specified IP address per second, and is in the range from 1 to 64000. With the ICMP flood attack protection enabled, the device enters the attack detection state. When the device detects that the sending rate of ICMP packets destined for the specified IP address constantly reaches or exceeds the specified action threshold, the device considers the IP address is under attack, enters the attack protection state, and takes protection actions as configured.<br>low rate-number: Sets the silence threshold for ICMP flood attack protection of the specified IP address. rate-number indicates the number of ICMP packets sent to the specified IP address per second, and is in the range from 1 to 64000. The default value of the silence threshold is 3/4 of the action threshold. If the device, when in the attack protection state, detects that the sending rate of ICMP packets destined for the specified IP address drops below the silence threshold, it considers that the attack is over, returns to the attack detection state, and stops the protection actions.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>8.<br>Original command:<br>**defense icmp-flood max-rate** *rate-number*<br>**undo defense icmp-flood max-rate**<br>Modified command:<br>**defense icmp-flood rate-threshold high** *rate-number* **[ low** *rate-number* **]**<br>**undo defense icmp-flood rate-threshold**<br>Module of the command: Security<br>Description: Change the parameter of **defense icmp-flood** from **max-rate** *rate-number* to **rate-threshold high** *rate-number* **[ low** *rate-number* **]**. Change the command of **undo defense icmp-flood** from **max-rate** to **rate-threshold.**<br>Parameters:<br>high rate-number: Sets the global action threshold for ICMP flood attack protection. rate-number indicates the number of ICMP packets sent to an IP address per second, and is in the range from 1 to 64000. With ICMP flood attack enabled, the device enters the attack detection state. When the device detects that the sending rate of ICMP packets destined for an IP address constantly reaches or exceeds the specified action threshold, the device considers the IP address is under attack, enters the attack protection state, and takes protection actions as configured.<br>low rate-number: Sets the global silence threshold for ICMP flood attack protection. rate-number indicates the number of ICMP packets sent to an IP address per second, and is in the range from 1 to 64000. If the device, when in the attack protection state, detects that the sending rate of ICMP packets destined for an IP address drops below the silence threshold, it considers that the attack to the IP address is over, returns to the attack |

| Item | Description |
| --- | --- |
| | detection state, and stops the protection actions.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>9.<br>Original command:<br>**defense syn-flood ip** *ip-address* **[ max-half-connections** *half-connections* \| **max-rate** *rate-number* **]**<br>**undo defense syn-flood ip** *ip-address* **[ max-half-connections** \| **max-rate ]**<br>Modified command:<br>**defense syn-flood ip** *ip-address* **rate-threshold high** *rate-number* **[ low** *rate-number* **]**<br>**undo defense syn-flood ip** *ip-address* **[ rate-threshold ]**<br>Module of the command: Security<br>Description: Change the parameter of **defense syn-flood ip** from **[ max-half-connections** *half-connections* \| **max-rate** *rate-number* **]** to **rate-threshold high** *rate-number* **[ low** *rate-number* **]**. Change the command of **undo defense syn-flood** from **[ max-half-connections** \| **max-rate ]** to **[ rate-threshold ].**<br>Parameters:<br>ip-address: IP address to be protected. This IP address cannot be a broadcast address, 127.0.0.0/8, a class D address, or a class E address.<br>high rate-number: Sets the action threshold for SYN flood attack protection of the specified IP address. rate-number indicates the number of SYN packets sent to the specified IP address per second, and is in the range 1 to 64000. With SYN flood attack protection enabled, the device enters the attack detection state. When the device detects that the sending rate of SYN packets destined for the specified IP address constantly reaches or exceeds the specified action threshold, the device considers the IP address is under attack, enters the attack protection state, and takes protection actions as configured.<br>low rate-number: Sets the silence threshold for SYN flood attack protection of the specified IP address. rate-number indicates the number of SYN packets sent to the specified IP address per second, and is in the range 1 to 64000. The default value of the silence threshold is 3/4 of the action threshold. If the device, when in the attack protection state, detects that the sending rate of SYN packets destined for the specified IP address drops below the silence threshold, it considers that the attack is over, returns to the attack detection state and stops taking the protection measures.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>10.<br>Original command:<br>**defense syn-flood { max-half-connections** *half-connections* \| **max-rate** *rate-number* **} ***<br>**undo defense syn-flood { max-half-connections** \| **max-rate }**<br>Modified command:<br>**defense syn-flood rate-threshold high** *rate-number* **[ low** *rate-number* **]**<br>**undo defense syn-flood rate-threshold**<br>Module of the command: Security |

| Item | Description |
| --- | --- |
| | Description: Change the parameter of **defense syn-flood** from **{ max-half-connections** *half-connections* \| **max-rate** *rate-number* **} *** to **rate-threshold high** *rate-number* **[ low** *rate-number* **]**. Change the command of **undo defense syn-flood** from **{ max-half-connections** \| **max-rate }** to **rate-threshold.** |
| | Parameters: |
| | high rate-number: Sets the global action threshold for SYN flood attack protection. rate-number indicates the number of SYN packets sent to an IP address per second, and is in the range 1 to 64000. With the SYN flood attack protection enabled, the device enters the attack detection state. When the device detects that the sending rate of SYN packets destined for an IP address constantly reaches or exceeds the specified action threshold, the device considers the IP address is under attack, enters the attack protection state, and takes protection actions as configured. |
| | low rate-number: Sets the global silence threshold for SYN flood attack protection. rate-number indicates the number of SYN packets sent to an IP address per second, and is in the range 1 to 64000. If the device, when in the attack protection state, detects that the sending rate of SYN packets destined for an IP address drops below the silence threshold, it considers that the attack to the IP address is over, returns to the attack detection state and stops the protection actions. |
| | Changes in default values: None. |
| | Changes in value ranges: None. |
| | 11. |
| | Original command: |
| | **defense udp-flood ip** *ip-address* **[ max-rate** *rate-number* **]** |
| | **undo defense udp-flood ip** *ip-address* **[ max-rate ]** |
| | Modified command: |
| | **defense udp-flood ip** *ip-address* **rate-threshold high** *rate-number* **[ low** *rate-number* **]** |
| | **undo defense udp-flood ip** *ip-address* **[ rate-threshold ]** |
| | Module of the command: Security |
| | Description: Change the parameter of **defense udp-flood ip** from **[ max-rate** *rate-number* **]** to **rate-threshold high** *rate-number* **[ low** *rate-number* **]**. Change the command of **undo defense udp-flood ip** from **[ max-rate ]** to **[ rate-threshold ].** |
| | Parameters: |
| | high rate-number: Sets the action threshold for UDP flood attack protection of the specified IP address. rate-number indicates the number of UDP packets sent to the specified IP address per second, and is in the range 1 to 64000. With the UDP flood attack protection enabled, the device enters the attack detection state. When the device detects that the sending rate of UDP packets destined for the specified IP address constantly reaches or exceeds the specified action threshold, the device considers the IP address is under attack, enters the attack protection state, and takes protection actions as configured. |
| | low rate-number: Sets the silence threshold for UDP flood attack protection of the specified IP address. rate-number indicates the number of UDP packets sent to the specified IP address per second, and is in the range 1 to 64000. The default value of the silence threshold is 3/4 of the action threshold. If the device, when in the attack protection state, detects that the sending rate of UDP packets destined for the specified IP |

| Item | Description |
| --- | --- |
| | address drops below the silence threshold, it considers that the attack is over, returns to the attack detection state, and stops the protection measures.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>12.<br>Original command:<br>**defense udp-flood max-rate** *rate-number*<br>**undo defense udp-flood max-rate**<br>Modified command:<br>**defense udp-flood rate-threshold high** *rate-number* **[ low** *rate-number* **]**<br>**undo defense udp-flood rate-threshold**<br>Module of the command: Security<br>Description: Change the parameter of **defense udp-flood** from Change the parameter of to **rate-threshold high** *rate-number* **[ low** *rate-number* **]**. Change the command of **undo defense udp-flood** from **max-rate** to **rate-threshold.**<br>Parameters:<br>high rate-number: Sets the global action threshold for UDP flood attack protection. rate-number indicates the number of UDP packets sent to an IP address per second, and is in the range 1 to 64000. With the UDP flood attack protection enabled, the device enters the attack detection state. When the device detects that the sending rate of UDP packets destined for an IP address constantly reaches or exceeds the specified action threshold, the device considers the IP address is under attack, enters the attack protection state, and takes protection actions as configured.<br>low rate-number: Sets the global silence threshold for UDP flood attack protection. rate-number indicates the number of UDP packets sent to an IP address per second, and is in the range 1 to 64000. If the device, when in the attack protection state, detects that the sending rate of UDP packets destined for an IP address drops below the silence threshold, it considers that the attack to the IP address is over, returns to the attack detection state, and stops the protection actions.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>13.<br>Original command:<br>**ospfv3** [ process-id ]<br>Modified command:<br>**ospfv3** [ process-id ] [ **vpn-instance** vpn-instance-name ]<br>Module of the command: OSPFv3<br>Description: Add the new parameter of [ **vpn-instance** vpn-instance-name ].<br>vpn-instance vpn-instance-name: Specifies an MPLS L3VPN. vpn-instance-name is a case-sensitive string of 1 to 31 characters. If no VPN is specified, the OSPFv3 process belongs to the public network. Support for this keyword and argument combination depends on the device model.<br>Changes in default values: None. |

| Item | Description |
| --- | --- |
| | Changes in value ranges: None.<br>14.<br>Original command:<br>**vad-on**<br>**undo vad-on**<br>Modified command:<br>**vad-on [ g723r53 \| g723r63 \| g729a \| g729r8 ] ***<br>**undo vad-on [ g723r53 \| g723r63 \| g729a \| g729r8 ] ***<br>Module of the command: Voice Entity<br>Description: Add the new parameters of **[ g723r53 \| g723r63 \| g729a \| g729r8 ] ***.<br>g723r53: Specifies the g723r53 codec.<br>g723r63: Specifies the g723r63 codec.<br>g729a: Specifies the g729a codec.<br>g729r8: Specifies the g729r8 codec.<br>Use the vad-on command to enable VAD.Use the undo vad-on command to disable VAD.<br>By default, VAD is disabled.If you execute the vad-on or undo vad-on command without specifying a codec, VAD for all codecs is enabled or disabled.The G.711 and G.726 codecs do not support VAD.The G.729br8 codec always supports VAD.<br>The VAD discriminates between silence and speech on a voice connection according to signal energies. VAD reduces the bandwidth requirements of a voice connection by not generating traffic during periods of silence in an active voice connection. Speech signals are generated and transmitted only when an active voice segment is detected. Researches show that VAD can save the transmission bandwidth by 50%.Related commands: cng-on.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>15.<br>Original command:<br>**display dns dynamic-host**<br>**display dns ipv6 dynamic-host**<br>Modified command:<br>**display dns host [ ip \| ipv6 \| naptr \| srv ]**<br>Module of the command: Domain name resolution<br>Description: Delete the commands of **display dns dynamic-host** and **display dns ipv6 dynamic-host**. Add a new command of **display dns host [ ip \| ipv6 \| naptr \| srv ]** instead.<br>View:<br>Any view<br>Parameters:<br>ip: Displays the dynamic cache information of type A queries. A type A query resolves a domain name to the mapped IPv4 address.<br>ipv6: Displays the dynamic cache information of type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address. |

| Item | Description |
| --- | --- |
| | For more information, see the Layer 3—IP Services Configuration Guide.<br>naptr: Displays the dynamic cache information of NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name. For more information, see the Voice Configuration Guide.<br>srv: Displays the dynamic cache information of SRV queries. An SRV query offers the domain name of a certain service site. For more information, see the Voice Configuration Guide.<br>\|: Filters command output by specifying a regular expression. For more information about regular expressions, see CLI configuration in the Fundamentals Configuration Guide.<br>begin: Displays the first line that matches the specified regular expression and all lines that follow.<br>exclude: Displays all lines that do not match the specified regular expression.<br>include: Displays all lines that match the specified regular expression.<br>regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.<br>Description:<br>Use the display dns host command to display the dynamic DNS cache information.<br>Without any keyword specified, the dynamic DNS cache information of all query types will be displayed.<br>Related commands: reset dns host.<br>Examples:<br># Display the dynamic DNS cache information of all query types.<br><Sysname> display dns host<br>No. Host TTL Type Reply Data<br>1 sample.com 3132 IP 192.168.10.1<br>2 sample.net 2925 IPv6 FE80::4904:4448<br>3 sip.sample.com 3122 NAPTR 100 10 u sip+E2U !^.*$!sip:info.se!i<br>4 website.tcp.sample.com 3029 SRV 10 10 8080 iis.sample.com<br>Changes in default values: None.<br>Changes in value ranges: None.<br>16.<br>Original command:<br>**reset dns dynamic-host**<br>**reset dns ipv6 dynamic-host**<br>Modified command:<br>**reset dns host [ ip \| ipv6 \| naptr \| srv ]**<br>Module of the command: Domain name resolution<br>Description: Delete the commands of **reset dns dynamic-host** and **reset dns ipv6 dynamic-host**. Add a new command of **reset dns host [ ip \| ipv6 \| naptr \| srv ]** instead.<br>View:<br>User view<br>Parameters: |

| Item | Description |
| --- | --- |
| | ip: Clears the dynamic cache information of type A queries. A type A query resolves a domain name to the mapped IPv4 address.<br>ipv6: Clears the dynamic cache information of type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address. For more information, see the Layer 3—IP Services Configuration Guide.<br>naptr: Clears the dynamic cache information of NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name. For more information, see the Voice Configuration Guide.<br>srv: Clears the dynamic cache information of SRV queries. An SRV query offers the domain name of a certain service site. For more information, see the Voice Configuration Guide.<br>Description:<br>Use the reset dns host command to clear information of the dynamic DNS cache.<br>Without any keyword specified, this command clears the dynamic DNS cache information of all query types.<br>Related commands: display dns host.<br>Examples:<br># Clear the dynamic DNS cache information of all query types.<br><Sysname> reset dns host<br>Changes in default values: None.<br>Changes in value ranges: None.<br>17.<br>Original command:<br>**nat outbound** [ *acl-number* ] [ **address-group** *group-number* [ **no-pat** [ **reversible** ] ] ] [ **track vrrp** *virtual-router-id* ]<br>**undo nat outbound** [ *acl-number* ] [ **address-group** *group-number* [ **no-pat** [ **reversible** ] ] ] [ **track vrrp** *virtual-router-id* ]<br>Modified command:<br>**nat outbound** [ *acl-number* ] [ **address-group** *group-number* [ **vpn-instance** *vpn-instance-name* ] [ **no-pat** [ **reversible** ] ] ] [ **track vrrp** *virtual-router-id* ]<br>**undo nat outbound** [ *acl-number* ] [ **address-group** *group-number* [ **vpn-instance** *vpn-instance-name* ] [ **no-pat** [ **reversible** ] ] ] [ **track vrrp** *virtual-router-id* ]<br>Module of the command: NAT<br>Description: Add a new parameter of **vpn-instance** *vpn-instance-name*. **vpn-instance** *vpn-instance-name:* Specifies the MPLS L3VPN to which the addresses of the address pool belong. The vpn-instance-name argument is a case-sensitive string of 1 to 31 characters. With this keyword and argument combination, inter-VPN access through NAT is supported. Without this keyword and argument combination, the addresses in the address pool do not belong to any VPN.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>18.<br>Original command:<br>**nat server protocol** *pro-type* **global** { *global-address* \| **interface** |

| Item | Description |
| --- | --- |
| | *interface-type interface-number* \| **current-interface** } *global-port1 global-port2* **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ]<br><br>**undo nat server protocol** *pro-type* **global** { *global-address* \| **interface** *interface-type interface-number* \| **current-interface** } *global-port1 global-port2* **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ]<br><br>**nat server** *index* **protocol** *pro-type* **global** { *global-address global-port1 global-port2* **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ] \| **current-interface** [ *global-port* ] **inside** *local-address* [ *local-port* ] [ **vpn-instance** *local-name* ] [ **remote-host** *host-address* ] [ **lease-duration** *lease-time* ] [ **description** *string* ] }<br><br>**undo nat server** *index* **protocol** *pro-type* **global** { *global-address global-port1 global-port2* **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ] \| **current-interface** [ *global-port* ] **inside** *local-address* [ *local-port* ] [ **vpn-instance** *local-name* ] [ **remote-host** *host-address* ] [ **lease-duration** *lease-time* ] [ **description** *string* ] }<br><br>Modified command:<br><br>**nat server protocol** *pro-type* **global** { *global-address* \| **interface** *interface-type interface-number* \| **current-interface** } *global-port1 global-port2* [ **vpn-instance** *global-name* ] **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ]<br><br>**undo nat server protocol** *pro-type* **global** { *global-address* \| **interface** *interface-type interface-number* \| **current-interface** } *global-port1 global-port2* [ **vpn-instance** *global-name* ] **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ]<br><br>**nat server** *index* **protocol** *pro-type* **global** { *global-address global-port1 global-port2* **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ] \| **current-interface** [ *global-port* ] **inside** *local-address* [ *local-port* ] [ **vpn-instance** *local-name* ] [ **remote-host** *host-address* ] [ **lease-duration** *lease-time* ] [ **description** *string* ] }<br><br>**undo nat server** *index* **protocol** *pro-type* **global** { *global-address global-port1 global-port2* **inside** *local-address1 local-address2 local-port* [ **vpn-instance** *local-name* ] [ **track vrrp** *virtual-router-id* ] \| **current-interface** [ *global-port* ] **inside** *local-address* [ *local-port* ] [ **vpn-instance** *local-name* ] [ **remote-host** *host-address* ] [ **lease-duration** *lease-time* ] [ **description** *string* ] }<br><br>Module of the command: NAT<br><br>Description: Add a new parameter of **vpn-instance** *global-name*. **vpn-instance** *global-name:* Specifies the MPLS L3VPN to which the advertised external network address belongs. The *global-name* argument is a case-sensitive string of 1 to 31 characters. Without this keyword and argument combination, the advertised external IP address does not belong to any VPN. Support for this keyword and argument combination depends on the device model.<br><br>Changes in default values: None.<br><br>Changes in value ranges: None.<br><br>19. |

| Item | Description |
| --- | --- |
| | Original command:<br>**nat static** [ *acl-number* ] *local-ip* [ **vpn-instance** *local-name* ] *global-ip*<br>**undo nat static** [ *acl-number* ] *local-ip* [ **vpn-instance** *local-name* ] *global-ip*<br>Modified command:<br>**nat static** [ *acl-number* ] *local-ip* [ **vpn-instance** *local-name* ] *global-ip* [ **vpn-instance** *global-name* ]<br>**undo nat static** [ *acl-number* ] *local-ip* [ **vpn-instance** *local-name* ] *global-ip* [ **vpn-instance** *global-name* ]<br>Module of the command:NAT<br>Description: Add a new parameter of **vpn-instance** *global-name*. **vpn-instance** *global-name:* case-sensitive string of 1 to 31 characters. Without this keyword and argument combination, the external IP address does not belong to any VPN.<br>Changes in default values: None.<br>Changes in value ranges: None. |
| CMW520-R2105P38 | |
| New commands | 1. Syntax<br>**fr fragment** [ *fragment-size* ] **end-to-end**<br>**undo fr fragment**<br>View<br>FR interface view<br>Parameters<br>*fragment-size*: Fragment size, which ranges from 16 bytes to 1600 bytes. This argument is 45 bytes by default.<br>Description<br>Use the fr fragment command to enable the FRF.12 packet fragmentation function for FR interface.<br>Use the undo fragment command to disable the FRF.12 packet fragmentation function.<br>By default, the FRF.12 packet fragmentation function is disabled for FR interface.<br>You cannot configure this command together with the fr traffic-sharping command.<br>Examples<br># Enable the FRF.12 packet fragmentation function with default fragment size of 45 bytes for the interface Serial2/0.<br><Sysname> system-view<br>[Sysname] interface serial 2/0<br>[Sysname-serial2/0] link-protocol fr<br>[Sysname-serial2/0] fr fragment end-to-end<br># Enable the FRF.12 packet fragmentation function with fragment size of 300 bytes for the interface Serial2/1.<br><Sysname> system-view<br>[Sysname] interface serial 2/1<br>[Sysname-serial2/1] link-protocol fr |

| Item | Description |
| --- | --- |
| | [Sysname-serial2/1] fr fragment 300 end-to-end<br>2. Syntax<br>**fips self-test**<br>View<br>User view<br>Parameters<br>None<br>Description<br>Use the **fips self-test** command to trigger a self-test on the password algorithms.<br>To verify whether the password algorithm modules operate normally, use this command to trigger a self-test on the password algorithms. The triggered self-test is the same as the automatic self-test when the device starts up.<br>If the self-test fails, the device automatically reboots.<br>Example<br># Trigger a self-test on the password algorithms.<br><Sysname> fips self-test<br>Self-tests are running. Please wait...<br>Self-tests succeeded.<br>3. Syntax<br>**crypto-digest sha256 file** *file-url*<br>View<br>User view<br>Parameters<br>**sha256**: Specifies the SHA-256 algorithm.<br>**file** *file-url*: Name of a file.<br>Description<br>Use the **crypto-digest** command to compute the digest of a specified file.<br>The computed digest is used to verify the correctness and integrity of the file to prevent the file from being tampered with. For example, you can use the command to compute the digest of the software image file of a device, and compare the digest with that on the web site of the device vendor to verify whether the file is valid.<br>Examples<br># Use the SHA-256 algorithm to compute the digest of the file 1.cfg.<br><Sysname> crypto-digest sha256 file 1.cfg<br>Computing digest...<br>SHA256 digest(1.cfg)=<br>7bcb92458222f91f9a09a807c4c4567efd4d5dc4e4abc06c2a741df7045433eb |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2105P31 | |

| Item | Description |
| --- | --- |
| New commands | 1. Syntax<br>**itf number** *number*<br>**undo itf number**<br>View<br>Serial interface view<br>Parameters<br>number *number*: Sets the number of interframe filling tags, which ranges from 0 to 14.<br>Description<br>Use the itf command to set the type of and the number of interframe filling tags on the serial interface.<br>Use the undo itf command to restore the default.<br>By default, the number of interframe filling tags is 4.<br>Examples<br># Set the number of interframe filling tags to five on interface E1 2/0.<br><Sysname> system-view<br>[Sysname] interface serial 2/0<br>[Sysname-Serial2/0] itf number 5<br>2. Syntax<br>**ipv6 neighbor stale-aging** *aging-time*<br>**undo ipv6 neighbor stale-aging**<br>View<br>System view<br>Parameters<br>*aging-time*: Age timer for ND entries in stale state, ranging from 1 to 24 hours.<br>Description<br>Use the ipv6 neighbor stale-aging command to set the age timer for ND entries in stale state.<br>Use the undo ipv6 neighbor stale-aging command to restore the default.<br>By default, the age timer for ND entries in stale state is four hours.<br>Examples<br># Set the age timer for ND entries in stale state to two hours.<br><Sysname> system-view<br>[Sysname] ipv6 neighbor stale-aging 2<br>3. Syntax<br>**next-server** *ip-address*<br>**undo next-server**<br>View<br>DHCP address pool view<br>Parameters<br>None<br>Description<br>Use the next-server command to specify the ip address of the follow-up |

| Item | Description |
| --- | --- |
| | server for DHCP client.<br>Use the undo next-server command to remove the ip address.<br>By default, the ip address of the follow-up server is not specified.<br>Examples<br># Specify the ip address of the follow-up server with 10.1.1.200.<br><Sysname> system-view<br>[Sysname] dhcp server ip-pool 0<br>[Sysname-dhcp-pool-0] next-server 10.1.1.200 |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2105P25 | |
| New commands | 1. Syntax<br>**fips mode enable**<br>**undo fips mode enable**<br>View<br>System view<br>Parameters<br>None<br>Description<br>Use the fips mode enable command to enable the FIPS mode.<br>Use the undo fips mode enable command to disable the FIPS mode.<br>By default, the FIPS mode is disabled.<br>The FIPS mode complies with the FIPS 140-2 standard.<br>After enabling the FIPS mode, you must restart the device to validate the configuration. Before restarting the device, complete the following configurations:<br>Specify the login username and password. The password must be at least 6-character long and must contain capital letters, lowercase letters, digits, and special characters.<br>Delete all digital certificates that use the MD5 algorithm.<br>Delete all DSA key pairs with a modulus less than 1024 bits and RSA key pairs.<br>After you restart the device, the device enters FIPS mode, and the following changes will occur:<br>FTP/TFTP server is disabled.<br>Telnet server is disabled.<br>HTTP server is disabled.<br>SNMPv1 and SNMPv2c are disabled. Only SNMPv3 is supported.<br>Only TLS1.0 is supported for the SSL server function.<br>The SSH server function does not provide SSHv1 client compatibility.<br>The device generates only RSA and DSA key pairs with a modulus between 1024 and 2048.<br>SSH, SNMPv3, IPsec, and SSL do not support the DES, RC4, and MD5 algorithms. |

| Item | Description |
| --- | --- |
| | Related commands: display fips status.<br>Examples<br># Enable FIPS mode.<br><Sysname> system-view<br>[Sysname] fips mode enable<br>2. Syntax<br>**display fips status**<br>View<br>Any view<br>Parameters<br>None<br>Description<br>Use the display fips status command to display the current FIPS mode.<br>Related commands: fips mode enable.<br>Examples<br># Display the current FIPS mode.<br><Sysname> system-view<br><Sysname> display fips status<br>FIPS mode is enabled |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2105P22 | |
| New commands | 1. Syntax<br>bandwidth bandwidth-value<br>undo bandwidth<br>View<br>Interface view<br>Parameters<br>bandwidth-value: Upper speed limit of an interface in kbps, in the range 1 to 4294967295.<br>Description<br>Use the bandwidth command to set the upper speed limit of an interface.<br>Use the undo bandwidth command to restore the default.<br>Examples<br># Set the upper speed limit of Ethernet 0/0 interface to 8192 kbps.<br><Sysname> system-view<br>[Sysname] interface ethernet 0/0<br>[Sysname-Ehternet0/0] bandwidth 8192 |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2105P12 | |

| Item | Description |
|---|---|
| New commands | 1. Syntax<br>**isdn carry channel-id once-only**<br>**undo isdn carry channel-id once-only**<br>View<br>ISDN interface view<br>Parameters<br>None<br>Description<br>Use the **isdn carry channel-id once-only** command to enable an ISDN interface to send out Alerting messages that do not carry the Channel-ID field.<br>Use the **undo isdn carry channel-id once-only** command to configure the interface to send out all Alerting messages with the Channel-ID field.<br>The **isdn carry channel-id once-only** command enables the compatibility with PBXs that cannot recognize the Channel-ID field in Alerting messages.<br>In a call process, if any message sent before the first Alerting message carries the Channel-ID field, the ISDN interface excludes the field from all outgoing Alerting messages. If not, the ISDN interface includes the Channel-ID field only in the first outgoing Alerting message.<br>By default, all outgoing ISDN messages carry the Channel-ID field. Use the default setting if your PBX can recognize the Channel-ID field in Alerting messages.<br>Examples<br># Enable interface BRI 2/0 to send out Alerting messages that do not carry the Channel-ID field.<br><Sysname> system-view<br>[Sysname] interface bri 2/0<br>[Sysname-Bri2/0] isdn carry channel-id once-only<br>Enabling outgoing Alerting messages that do not carry the Channel-ID field<br>By default, the router sends out all outgoing ISDN messages with the Channel-ID field. If the remote PBX cannot recognize the Channel-ID field in Alerting messages, you must enable the ISDN interface to send out Alerting messages that do not carry the Channel-ID field. In any other case, use the default setting.<br>Follow these steps to enable an ISDN interface to send out Alerting messages that do not carry the Channel-ID field:<br>To do… Use the command… Description<br>Enter system view system-view -<br>Enter interface view interface interface-type - interface-number<br>Enable Alerting messages that do not carry the Channel-ID field isdn carry channel-id once-only Optional. By default, all outgoing ISDN messages carry the Channel-ID field.<br>2. Syntax<br>**modem response timer** *time* **auto-recovery** *threshold* |

| Item | Description |
| --- | --- |
| | **undo modem response**<br>View<br>Cellular interface view<br>Parameters<br>time: Timeout period (in seconds), which ranges from 0 to 300 and defaults to 10.<br>threshold: Maximum number of continuous response failures of the 3G Modem. After the threshold is reached, the system automatically resets the 3G modem. This argument ranges from 0 to 10 and defaults to 3. When this argument is set to 0, the automatic recovery function is disabled.<br>Description<br>Use the **modem response timer** *time* **auto-recovery** *threshold* command to configure the timeout period of waiting for responses from the 3G modem after the system sending AT commands to the 3G modem, and configure the maximum number of continuous response failures of the 3G Modem. After the threshold is reached, the system automatically resets the 3G modem.<br>Use the **undo modem response** command to restore the default.<br>Examples<br># Configure the timeout period of waiting for responses from the 3G modem as 20 seconds after the system sends AT commands to the 3G modem, and configure the maximum number of continuous response failures of the 3G Modem as 4.<br><Sysname> system-view<br>[Sysname] interface cellular 0/0<br>[Sysname-Cellular0/0] modem response timer 20 auto-recovery 4<br>3G modems fall into the following types: USB 3G modem and SIC-3G interface module. |
| Removed commands | None |
| Modified commands | None |
| CMW520-R2105P06 | |
| New commands | Notes: New commands of 6VPE Please refer to 6VPE feature.zip.<br>Other new commands: None. |
| Removed commands | 1. Syntax:<br>**ppp ignore match-next-hop**<br>**undo ppp ignore match-next-hop**<br>Module of the command: PPP<br>Description: This command is no more applicable to the new forward flow.<br>Notes: Deleted commands of 6VPE Please refer to 6VPE feature.zip. |
| Modified commands | 1.Original command:<br>**info-center loghost** { **ipv6** host-ipv6-address }[ **vpn-instance** vpn-instance-name ] { host-ipv4-address} [ **port** port-number ] [ **channel** { channel-number \| channel-name } \| **facility** local-number ] *<br>**undo info-center loghost ipv6** {host-ipv6-address \| **vpn-instance** vpn-instance-name ] host-ipv4-address } |

| Item | Description |
| --- | --- |
| | Modified command:<br>**info-center loghost** [ **vpn-instance** vpn-instance-name ] { host-ipv4-address \| **ipv6** host-ipv6-address } [ **port** port-number ] [ **channel** { channel-number \| channel-name } \| **facility** local-number ] *<br>**undo info-center loghost** [ **vpn-instance** vpn-instance-name ] { host-ipv4-address \| **ipv6** host-ipv6-address }<br>Module of the command: Information Center<br>Description: Just the order of [ **vpn-instance** vpn-instance-name ] { host-ipv4-address} and { **ipv6** host-ipv6-address }.<br>**vpn-instance** *vpn-instance-name*: Specifies the MPLS L3VPN to which the log host belongs, where *vpn-instance-name* is a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this keyword and argument combination.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.Original command:<br>**userlog nat export host** { ipv4-address \| **ipv6** ipv6-address } udp-port<br>**undo userlog nat exporthost** { ipv4-address \| **ipv6** ipv6-address } udp-port<br>Modified command:<br>**userlog nat export** [ **vpn-instance** *vpn-instance-name* ] **host** { ipv4-address \| **ipv6** ipv6-address } udp-port<br>**undo userlog nat export** [ **vpn-instance** *vpn-instance-name* ] **host** { ipv4-address \| **ipv6** ipv6-address } udp-port<br>Module of the command: NAT<br>Description: Add new parameter of [ **vpn-instance** *vpn-instance-name* ]. **vpn-instance** *vpn-instance-name:* Specifies the MPLS L3 VPN that the NAT log server belongs to. The *vpn-instance-name* argument is a case sensitive string of 1 to 31 characters. If the NAT log server is on the public network, do not specify this keyword and argument combination.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>3.Original command:<br>**key** { **accounting** \| **authentication** \| **authorization** } *string*<br>**undo key** { **accounting** \| **authentication** \| **authorization** } *string*<br>Modified command:<br>**key** { **accounting** \| **authentication** \| **authorization** } *string*<br>**undo key** { **accounting** \| **authentication** \| **authorization** } *string*<br>Module of the command: AAA<br>Description: Change the range of *string*: Shared key, a case-sensitive string of 1 to 255 (the old version is 1to 64) characters.<br>Changes in default values: None.<br>Changes in value ranges: Change the range of *string*: Shared key, a case-sensitive string of 1 to 255 (the old version is 1to 64) characters.<br>Notes: Modified commands of 6VPE Please refer to 6VPE feature.zip. |
| CMW520-R2105P02 | |
| New commands | 1.Syntax<br>**isdn service [ audio \| data \| speech ]** |

| Item | Description |
| --- | --- |
| | **undo isdn service**<br>View<br>ISDN interface view (voice interface)<br>Parameters<br>**audio**: Specifies the 3.1 kHz audio service.<br>**data**: Specifies the Unrestricted digital information service.<br>**speech**: Specifies the speech service.<br>Description<br>Use the **isdn service** command to specify the service type in the ISDN Bearer Compatibility Capability signalling messages.<br>Use the **undo isdn service** command to restore the default service type in the ISDN Bearer Compatibility Capability signalling messages.<br>By default, the service type in the ISDN Bearer Compatibility Capability signalling messages is speech.<br>This command is available on only voice interfaces such as BSV, VE1, and VT1 interfaces.<br>Examples<br># Specify the service type as audio in the ISDN Bearer Compatibility Capability signalling messages.<br><Sysname> system-view<br>[Sysname] interface bri 1/0<br>[Sysname-Bri1/0] isdn service audio |
| Removed commands | None |
| Modified commands | 1.Original command:<br>**nat aging-time** { **dns** \| **ftp-ctrl** \| **ftp-data** \| **icmp** \| **pptp** \| **tcp** \| **tcp-fin** \| **tcp-syn** \| **udp** } *seconds*<br>**undo nat aging-time** { **dns** \| **ftp-ctrl** \| **ftp-data** \| **icmp** \| **pptp** \| **tcp** \| **tcp-fin** \| **tcp-syn** \| **udp** } [ *seconds* ]<br>Modified command:<br>**nat aging-time** { **dns** \| **ftp-ctrl** \| **ftp-data** \| **icmp** \| **no-pat** \| **pptp** \| **tcp** \| **tcp-fin** \| **tcp-syn** \| **udp** } *seconds*<br>**undo nat aging-time** { **dns** \| **ftp-ctrl** \| **ftp-data** \| **icmp** \| **no-pat** \| **pptp** \| **tcp** \| **tcp-fin** \| **tcp-syn** \| **udp** } [ *seconds* ]<br>Module of the command: NAT<br>Description: Add new parameter of **no-pat**: Specify the NAT aging-time for NO-PAT. 240 seconds for NO-PAT.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.Original command:<br>**display current-configuration** [ [ **configuration** [ *configuration* ] \| **controller** \| **interface** [ *interface-type* ] [ *interface-number* ] ] [ **by-linenum** ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ] ]<br>Modified command:<br>**display current-configuration** [ [ **configuration** [ *configuration* ] \| **controller** \| **interface** [ *interface-type* ] [ *interface-number* ] \| **exclude** *modules* ] [ **by-linenum** ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ] ] |

| Item | Description |
| --- | --- |
| | Module of the command: Management.<br>Description: Add new parameter of **exclude** *modules*: Displays the configuration information of the modules other than the specified modules. You can specify multiple modules at one time, with spaces to separate them. For example, the **display current-configuration exclude a b** command displays the configuration information of the modules other than modules **a** and **b**. Currently, the *modules* argument can be **acl** and **acl6**. You can specify either or both of them to display the configuration information of modules other than the ACL module, the IPv6 ACL module, or both of them.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>3.Original command:<br>**if-match community** { { *basic-community-list-number* } [ **whole-match** ] \| *adv-community-list-number* }&<1-16><br>**undo if-match community** [ *basic-community-list-number* } [ **whole-match** ] \| *adv-community-list-number* ]&<1-16><br>Modified command:<br>**if-match community** { { *basic-community-list-number* \| *comm-list-name* } [ **whole-match** ] \| *adv-community-list-number* }&<1-16><br>**undo if-match community** [ *basic-community-list-number* \| *comm-list-name* } [ **whole-match** ] \| *adv-community-list-number* ]&<1-16><br>Module of the command: Routing policy.<br>Description: Add new parameter of *comm-list-name*: Community list name, a string of 1 to 31 characters, which can contain letters, numbers, and signs.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>4.Original command:<br>**display bgp routing-table community-list** { { *basic-community-list-number* } [ **whole-match** ] \| *adv-community-list-number* }&<1-16> [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>Modified command:<br>**display bgp routing-table community-list** { { *basic-community-list-number* \| *comm-list-name* } [ **whole-match** ] \| *adv-community-list-number* }&<1-16> [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>Module of the command: BGP<br>Description: Add new parameter of *comm-list-name*: Community list name, a string of 1 to 31 characters (not all are numbers).<br>Changes in default values: None.<br>Changes in value ranges: None.<br>5.Original command:<br>**ip route-static** *dest-address* { *mask* \| *mask-length* } { *next-hop-address* [ **track** *track-entry-number* ] \| *interface-type interface-number* [ *next-hop-address* ] [ **bfd** { **control-packet** \| **echo-packet** } ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* [ **track** *track-entry-number* ] } [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ **description** *description-text* ]<br>**undo ip route-static** *dest-address* { *mask* \| *mask-length* } |

| Item | Description |
| --- | --- |
| | [ *next-hop-address* \| *interface-type interface-number* [ *next-hop-address* ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* ] [ **preference** *preference-value* ]<br>**ip route-static vpn-instance** *s-vpn-instance-name*&<1-6> *dest-address* { *mask* \| *mask-length* } { *next-hop-address* [ **track** *track-entry-number* ] [ **public** ] \| *interface-type interface-number* [ *next-hop-address* ] [ **bfd** { **control-packet** \| **echo-packet** } ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* [ **track** *track-entry-number* ] } [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ **description** *description-text* ]<br>**undo ip route-static vpn-instance** *s-vpn-instance-name*&<1-6> *dest-address* { *mask* \| *mask-length* } [ *next-hop-address* [ **public** ] \| *interface-type interface-number* [ *next-hop-address* ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* ] [ **preference** *preference-value* ]<br>Modified command:<br>**ip route-static** *dest-address* { *mask* \| *mask-length* } { *next-hop-address* [ **track** *track-entry-number* ] \| *interface-type interface-number* [ *next-hop-address* ] [ **bfd** { **control-packet** \| **echo-packet** } ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* [ **track** *track-entry-number* ] } [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ **permanent** ] [ **description** *description-text* ]<br>**undo ip route-static** *dest-address* { *mask* \| *mask-length* } [ *next-hop-address* \| *interface-type interface-number* [ *next-hop-address* ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* ] [ **preference** *preference-value* ]<br>**ip route-static vpn-instance** *s-vpn-instance-name*&<1-6> *dest-address* { *mask* \| *mask-length* } { *next-hop-address* [ **track** *track-entry-number* ] [ **public** ] \| *interface-type interface-number* [ *next-hop-address* ] [ **bfd** { **control-packet** \| **echo-packet** } ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* [ **track** *track-entry-number* ] } [ **preference** *preference-value* ] [ **tag** *tag-value* ] [ **permanent** ] [ **description** *description-text* ]<br>**undo ip route-static vpn-instance** *s-vpn-instance-name*&<1-6> *dest-address* { *mask* \| *mask-length* } [ *next-hop-address* [ **public** ] \| *interface-type interface-number* [ *next-hop-address* ] \| **vpn-instance** *d-vpn-instance-name next-hop-address* ] [ **preference** *preference-value* ]<br>Module of the command: Static Routing.<br>Description: Add new parameter of **permanent**: Specifies the route as a permanent static route. If the outgoing interface is down, the permanent static route is still active.<br>Notes: Do not specify the **permanent** keyword together with the **bfd** or **track** keyword.<br>Changes in default values: None.<br>Changes in value ranges: None. |
| CMW520-R2105 | |
| New commands | 1. Syntax<br>**bidir-pim enable**<br>**undo bidir-pim enable**<br>View<br>Public network PIM view, VPN instance PIM view<br>Parameters<br>None |

| Item | Description |
|---|---|
| | Description<br>Use the **bidir-pim enable** command to enable BIDIR-PIM.<br>Use the **undo bidir-pim enable** command to disable BIDIR-PIM.<br>By default, BIDIR-PIM is disabled.<br>Examples<br># Enable BIDIR-PIM on the public network.<br><Sysname> system-view<br>[Sysname] pim<br>[Sysname-pim] bidir-pim enable<br>2. Syntax<br>**display pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] **df-info** [ *rp-address* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>View<br>Any view<br>Parameters<br>**all-instance**: Specifies all instances.<br>**vpn-instance** *vpn-instance-name*: Specifies a VPN instance. A VPN instance name is a case sensitive string of up to 31 characters and must not contain any space.<br>*rp-address*: Specifies the RP address of BIDIR-PIM.<br>\|: Filters command output by specifying a regular expression. For more information about regular expressions, see *CLI* in the *Fundamentals Configuration Guide*.<br>**begin**: Displays the first line that matches the specified regular expression and all lines that follow.<br>**exclude**: Displays the lines that do not match the specified regular expression.<br>**include**: Displays all lines that match the specified regular expression.<br>*regular-expression*: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.<br>Description<br>Use the **display pim df-info** command to display the DF information of BIDIR-PIM.<br>If neither **all-instance** nor **vpn-instance** is specified, this command displays the DF information of BIDIR-PIM on the public network.<br>Examples<br># Display the DF information of BIDIR-PIM on the public network.<br><Sysname> display pim df-info<br>VPN-Instance: public net<br>RP Address: 1.1.1.1<br>Interface State DF-Pref DF-Metric DF-Uptime DF-Address<br>Eth1/1 Win 100 1 01:24:09 192.168.2.1(local)<br>Ser2/1 Win 100 1 01:24:09 10.110.1.2(local)<br>Ser2/2 Loss 0 0 01:23:12 10.110.2.2<br>Display pim df-info command output description:<br>Field Description |

| Item | Description |
|---|---|
| | VPN-Instance: public net Public network |
| | RP Address BIDIR-PIM RP address |
| | Interface Interface type and number |
| | State DF election state: |
| | Win |
| | Lose |
| | DF-Pref Route priority of DF |
| | DF-Metric Route metric of DF |
| | 3. Syntax |
| | **display multicast** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] **forwarding-table df-info** [ *rp-address* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ] |
| | View |
| | Any view |
| | Parameters |
| | all-instance: Specifies all MPLS L3VPN instances. |
| | vpn-instance vpn-instance-name: Specifies an MPLS L3VPN instance, where vpn-instance-name is a case sensitive string of 1 to 31 characters. |
| | rp-address: RP address of BIDIR-PIM. |
| | slot slot-number: Displays the DF information of the multicast forwarding table for the card specified by its slot number. If no slot is specified, the command displays the DF information of the multicast forwarding table for the main processing board. (On a distributed device) |
| | chassis chassis-number slot slot-number: Displays the DF information of the multicast forwarding table for a card on an IRF member device. The chassis-number argument refers to the ID of the IRF member device, and the slot-number argument refers to the number of the slot where the card resides. If this keyword and argument combination is not configured, the command displays the DF information of the multicast forwarding tables for all main processing boards in the IRF member device. (On a distributed IRF member device) |
| | \|: Filters command output by specifying a regular expression. For more information about regular expressions, see CLI in the Fundamentals Configuration Guide. |
| | begin: Displays the first line that matches the specified regular expression and all lines that follow. |
| | exclude: Displays the lines that do not match the specified regular expression. |
| | include: Displays all lines that match the specified regular expression. |
| | regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters. |
| | Description |
| | Use the display multicast forwarding-table df-info command to display the DF information of the multicast forwarding table. |
| | If neither all-instance nor vpn-instance is specified, this command displays the DF information for the public network. |
| | Examples |
| | # Display the DF information of the multicast forwarding table for the public network. |

| Item | Description |
|---|---|

<Sysname> display multicast forwarding-table df-info

Multicast DF information of VPN-Instance: public net

Total 1 RP

Total 1 RP matched

00001. RP Address: 1.1.1.1

MID: 0, Flags: 0x100000:0

Uptime: 00:08:32

RPF interface: Ethernet1/1

List of 1 DF interfaces:

1: Ethernet1/2

Display multicast forwarding-table df-info command output description:

| Field | Description |
|---|---|
| Multicast DF information of VPN-Instance: public net | DF information of the multicast forwarding table for the public network |
| Total 1 RP | Total number of RPs |
| Total 1 RP matched | Total number of matched RPs |
| 00001 | Sequence number of the RP |
| MID | ID of the RP. Each RP has a unique MID. |
| Flags | Current state of the RP. Different bits are used to indicate different states of an RP. |
| Uptime | Length of time for which the RP has been up, in hours:minutes:seconds |
| RPF interface | RPF interface to the RP |
| List of 1 DF interfaces | DF interface list |

4. Syntax

**bidir-pim enable**

**undo bidir-pim enable**

View

IPv6 PIM view

Parameters

None

Description

Use the bidir-pim enable command to enable IPv6 BIDIR-PIM.

Use the undo bidir-pim enable command to disable IPv6 BIDIR-PIM.

By default, IPv6 BIDIR-PIM is disabled.

Examples

# Enable IPv6 BIDIR-PIM.

<Sysname> system-view

[Sysname] pim ipv6

[Sysname-pim6] bidir-pim enable

5. Syntax

**display pim ipv6 df-info** [ *rp-address* ] [ | { **begin** | **exclude** | **include** }

| Item | Description |
|---|---|
| | *regular-expression* ]<br>View<br>Any view<br>Parameters<br>rp-address: Specifies the RP address of IPv6 BIDIR-PIM.<br>\|: Filters command output by specifying a regular expression. For more information about regular expressions, see CLI in the Fundamentals Configuration Guide.<br>begin: Displays the first line that matches the specified regular expression and all lines that follow.<br>exclude: Displays the lines that do not match the specified regular expression.<br>include: Displays all lines that match the specified regular expression.<br>regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.<br>Description<br>Use the display pim ipv6 df-info command to display the DF information of IPv6 BIDIR-PIM.<br>Examples<br># Display the DF information of IPv6 BIDIR-PIM.<br><Sysname> display pim df-info<br>RP Address: 2010::1<br>Interface State DF-Pref DF-Metric DF-Uptime DF-Address<br>Eth1/1 Win 100 1 01:24:09 2001::1(local)<br>Ser2/1 Win 100 1 01:24:09 1002::2(local)<br>Ser2/2 Loss 0 0 01:23:12 2002::2<br>Display pim ipv6 df-info command output description:<br>Field Description<br>RP Address IPv6 BIDIR-PIM RP address<br>Interface Interface type and number<br>State DF election state, which can be Win or Loss<br>DF-Pref Route priority of DF<br>DF-Metric Route metric of DF<br>(6)<br>Syntax<br>**display multicast ipv6 forwarding-table df-info** [ *rp-address* ] [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>View<br>Any view<br>Parameters<br>rp-address: RP address of IPv6 BIDIR-PIM.<br>slot slot-number: Displays the DF information of the IPv6 multicast forwarding table for the card specified by its slot number. If no slot is specified, the command displays the DF information of the IPv6 multicast forwarding table for the main processing board. (On a distributed device) |

| Item | Description |
|---|---|
| | chassis chassis-number slot slot-number: Displays the DF information of the IPv6 multicast forwarding table for a card on an IRF member device. The chassis-number argument refers to the ID of the IRF member device, and the slot-number argument refers to the number of the slot where the card resides. If this keyword and argument combination is not configured, the command displays the DF information of the IPv6 multicast forwarding tables for all main processing boards in the IRF member device. (On a distributed IRF member device) |
| | \|: Filters command output by specifying a regular expression. For more information about regular expressions, see CLI in the Fundamentals Configuration Guide. |
| | begin: Displays the first line that matches the specified regular expression and all lines that follow. |
| | exclude: Displays the lines that do not match the specified regular expression. |
| | include: Displays all lines that match the specified regular expression. |
| | regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters. |
| | Description |
| | Use the display multicast ipv6 forwarding-table df-info command to display the DF information of the IPv6 multicast forwarding table. |
| | Examples |
| | # Display the DF information of the IPv6 multicast forwarding table. |
| | <Sysname> display multicast ipv6 forwarding-table df-info |
| | Multicast DF information |
| | Total 1 RP |
| | Total 1 RP matched |
| | 00001. RP Address: 2010::1 |
| | MID: 0, Flags: 0x100000:0 |
| | Uptime: 00:08:32 |
| | RPF interface: Ethernet1/1 |
| | List of 1 DF interfaces: |
| | 1: Ethernet1/2 |
| | Display multicast ipv6 forwarding-table df-info command output description: |

| Field | Description |
|---|---|
| Multicast DF information | DF information of the IPv6 multicast forwarding table |
| Total 1 RP | Total number of RPs |
| Total 1 RP matched | Total number of matched RPs |
| 00001 | Sequence number of the RP |
| MID | ID of the RP. Each RP has a unique MID. |
| Flags | Current state of the RP. Different bits are used to indicate different states of an RP. |
| Uptime | Length of time for which the RP has been up, in hours:minutes:seconds |
| RPF interface | RPF interface to the RP |

| Item | Description |
| --- | --- |
| | List of 1 DF interfaces DF interface list |
| Removed commands | None |
| Modified commands | 1. Original command:<br>**cid ring** { **0** \| **1** \| **2** }<br>**undo cid ring**<br>Modified command:<br>**cid ring** { **0** \| **1** \| **2** } [ *times* ]<br>**undo cid ring**<br>Module of the command: Voice<br>Description: Add a new parameter [ times ].<br>times: Ring count after the CID check before the FXO line goes off-hook. The value is in the range 0 to 5. The greater the value, the later the FXO line goes off-hook.<br>Use the cid ring command to configure the time for CID check and after the CID check, the number of rings the FXO line receives before going off-hook.<br>Use the undo cid ring command to restore the default.<br>By default, CID check is performed between the first and the second rings and the FXO line goes off-hook as soon as the check completes, that is, cid ring 1 0.<br>Caution: The configuration of the cid ring command loses effect after the execution of the undo cid receive command in voice subscriber line view, and the phone goes off-hook as soon as the FXO interface detects the first ring.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>2.Original command:<br>**dtmf sensitivity-level** { **high** \| **low** \| **medium** }<br>**undo dtmf sensitivity-level**<br>Modified command:<br>**dtmf sensitivity-level** { **high** \| **low** \| **medium** [ **frequency-tolerance** *value* ] }<br>**undo dtmf sensitivity-level**<br>Module of the command: Voice<br>Description: Add a new parameter [ frequency-tolerance value ].<br>frequency-tolerance value: Absolute frequency deviation (in percentage) when the DTMF detection sensitivity level is set to medium. The value is in the range 1.0 to 5.0 and defaults to 2.0. The greater the value, the higher the probability of false detection.<br>Use the dtmf sensitivity-level command to set the DTMF detection sensitivity level and the absolute frequency deviation when the DTMF detection sensitivity level is set to medium.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>3. Original command:<br>**display pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] |

| Item | Description |
| --- | --- |
| | **routing-table** [ *group-address* [ **mask** { *mask-length* \| *mask* } ] \| *source-address* [ **mask** { *mask-length* \| *mask* } ] \| **incoming-interface** [ *interface-type interface-number* \| **register** ] \| **outgoing-interface** { **include** \| **exclude** \| **match** } { *interface-type interface-number* \| **register** } \| **mode** *mode-type* \| **flags** *flag-value* \| **fsm** ] * [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>Modified command:<br>**display pim** [ **all-instance** \| **vpn-instance** *vpn-instance-name* ] **routing-table** [ *group-address* [ **mask** { *mask-length* \| *mask* } ] \| *source-address* [ **mask** { *mask-length* \| *mask* } ] \| **incoming-interface** [ *interface-type interface-number* \| **register** ] \| **outgoing-interface** { **include** \| **exclude** \| **match** } { *interface-type interface-number* \| **register** } \| **mode** *mode-type* \| **flags** *flag-value* \| **fsm** ] * [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>Module of the command: PIM<br>Description: Add a new value of *flag-value*:<br>□ bidir: Specifies PIM routing entries created by BIDIR-PIM.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>4. Original command:<br>**static-rp** *rp-address* [ *acl-number* ] [ **preferred** ]<br>**undo static-rp** *rp-address*<br>Modified command:<br>**static-rp** *rp-address* [ *acl-number* ] [ **preferred** ] [ **bidir** ]<br>**undo static-rp** *rp-address*<br>Module of the command: PIM<br>Description: Add a new parameter of [ bidir ]:<br>bidir: Configures the static RP to serve multicast groups in BIDIR-PIM. Without this argument, the static RP serves groups in PIM-SM.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>5. Original command:<br>**static-rp** *ipv6-rp-address* [ *acl6-number* ] [ **preferred** ]<br>**undo static-rp** *ipv6-rp-address*<br>Modified command:<br>**static-rp** *ipv6-rp-address* [ *acl6-number* ] [ **preferred** ] [ **bidir** ]<br>**undo static-rp** *ipv6-rp-address*<br>Module of the command: PIM<br>Description: Add a new parameter of [ bidir]:<br>**bidir**: Configures the static RP to serve multicast groups in IPv6 BIDIR-PIM. Without this argument, the static RP serves groups in IPv6 PIM-SM.<br>Changes in default values: None.<br>Changes in value ranges: None.<br>6. Original command:<br>**display pim ipv6 routing-table** [ *ipv6-group-address* [ *prefix-length* ] \| *ipv6-source-address* [ *prefix-length* ] \| **incoming-interface** [ *interface-type interface-number* \| **register** ] \| **outgoing-interface** { **include** \| **exclude** \| |

| Item | Description |
| --- | --- |
| | **match** } { *interface-type interface-number* \| **register** } \| **mode** *mode-type* \| **flags** *flag-value* \| **fsm** ] * [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>Modified command:<br>**display pim ipv6 routing-table** [ *ipv6-group-address* [ *prefix-length* ] \| *ipv6-source-address* [ *prefix-length* ] \| **incoming-interface** [ *interface-type interface-number* \| **register** ] \| **outgoing-interface** { **include** \| **exclude** \| **match** } { *interface-type interface-number* \| **register** } \| **mode** *mode-type* \| **flags** *flag-value* \| **fsm** ] * [ \| { **begin** \| **exclude** \| **include** } *regular-expression* ]<br>Module of the command: PIM<br>Description: Add a new value of *flag-value*:<br>□ bidir: Specifies IPv6 multicast routing entries created by IPv6 BIDIR-PIM.<br>Changes in default values: None.<br>Changes in value ranges: None. |

# MIB updates

Table 14 MIB updates

| Item | MIB file | Module | Description |
| --- | --- | --- | --- |
| CMW520-R2209 | | | |
| New | None | None | None |
| Modified | rfc1213.mib | RFC1213-MIB | Modified all the descriptions of<br>ipv6InterfaceTable, ipSystemStatsTable, ipIfStatsTable, ipAddressPrefixTable, ipAddressTable, ipNetToPhysicalTable, ipv6ScopeZoneIndexTable, ipDefaultRouterTable, ipv6RouterAdvertTable, icmpStatsTable and icmpMsgStatsTable to Not supported |
| CMW520-R2207P02 | | | |
| New | rfc2515-atm.mib | ATM-MIB | Add ATMIMA to the table of atmInterfaceMaxActiveVciBits |
| | rfc2515-atm.mib | ATM-MIB | Add GBIS and ATMIMA to the table of atmInterfaceMaxVccs |
| | rfc1213.mib | RFC1213-MIB | Modified description of ifSpeed from an estimate of the interface's current bandwidth in bits per second to configured by the bandwidth command, and it's different in various types of interfaces by default. |
| | hh3c-dar.mib | HH3C-DAR-MIB | Modified the oid of hh3cDarStatisticsTable |
| Modified | None | None | None |

| Item | MIB file | Module | Description |
|---|---|---|---|
| CMW520-R2207 | | | |
| New | hh3c-nqa.mib | HH3C-NQA-MIB | Add hh3cNqaStatisticsReactionTable and h3cNqaReactionTable |
| | hh3c-nqa.mib | HH3C-NQA-MIB | Add such TRAPs in HH3C-NQA-MIB: hh3cNqaProbeTimeOverThreshold, hh3cNqaJitterRTTOverThreshold, hh3cNqaProbeFailure, hh3cNqaJitterPacketLoss, hh3cNqaJitterSDOverThreshold, hh3cNqaJitterDSOverThreshold, hh3cNqaICPIFOverThreshold and hh3cNqaMOSOverThreshold |
| | Hh3c-e1t1vi.mib | HH3C-E1T1VI-MIB | Add hh3cE1T1VITrapTimeSlotEnable |
| | hh3c-e1.mib | HH3C-E1-MIB | Add hh3ce1FcmChannelIndex and hh3ce1TimeSlotSetTable |
| Modified | hh3c-splat-mstp.mib | HH3C-LswMSTP-MIB | Modified the description of hh3cdot1sMstAdminFormatSelector. Changed the value range from [0..255] to 0 |
| | hh3c-dhcps.mib | HH3C-DHCPS-MIB | Modified the description of hh3cDHCPSGlobalPoolLeaseUnlimited. Added the value can't be set to 0 |
| | rfc1657-bgp4.mib | BGP4-MIB | Modified the PDS of bgpeerAdminStatus, bgpPeerHoldTimeConfigured, bgpPeerKeepAliveConfigured, bgpPeerMinASOriginationInterval and bgpPeerMinRouteAdvertisementInterval |
| | Hh3c-posa.mib | HH3C-POSA-MIB | Modified the PDS of hh3cPosaTerminalTable and hh3cPosaAppTable |

# Configuration changes

None.

# Open problems and workarounds

None.

# List of resolved problems

## Resolved problems in CMW520-R2209

### RTD59161

- First found in CMW520-R2207P38
- Condition: The router runs NAT function, and there are several NAT outbound commands at the interface of the router.
- Description: When transmits some UDP packets, the router will reboot abnormally.

### RTD58793

- First found in CMW520-R2207
- Condition: Run NQA function in the Multilink PPP link with several physical interfaces.
- Description: The result of NQA was inaccurate.

### RTD58598

- First found in CMW520-R2207
- Condition: The aysnc interface of the router works at flow mode.
- Description: The line protocol status of the async interface is always down.

### RTD59306

- First found in CMW520-R2207P45
- Condition: Run OSPF protocol in the router.
- Description: OSPF Area 0 ABR does not generate default to stub when no neighbor in Area 0.

## Resolved problems in CMW520-R2207P45

### RTD58789

- First found in CMW520-R2207
- Condition: The interface of the router set PPP protocol and CHAP authentication.
- Description: If the router received challenge more than 16 bytes, the PPP CHAP authentication failed.

### RTD58508

- First found in CMW520-R2207P14
- Condition: None.

- Description: The router can't identify the INARP packets with filled information, so the router failed to parse the IP address.

RTD57556

- First found in CMW520-R2207P14
- Condition: The CPU usage of the router was high.
- Description: Because the BGP timer of the router was inaccurate, the BGP neighbors were UP and DOWN again and again.

# Resolved problems in CMW520-R2207P38

RTD58234

- First found in CMW520-R2207
- Condition: Insert a pseudo fiber module to a port of an HP A-MSR router.
- Description: The port will be shut down.

RTD57850

- First found in CMW520-R2207P14
- Condition: None.
- Description: There wasn't the command to adjust the cable attenuation parameters at the IMA-T1 interface of the router.

RTD57858

- First found in CMW520-R2207P14
- Condition: None.
- Description: The pulse shape of IMA-T1 interface was too low.

RTD58297

- First found in CMW520-R2207P14
- Condition: None.
- Description: The pulse shape of SIC-EPRI interface has overshot /undershot.

RTD58164

- First found in CMW520-R2207P14
- Condition: None.
- Description: The pulse shape of IMA-E1 interface was too low.

RTD57892

- First found in CMW520-R2207P14
- Condition: The router as VOICE gateway connected with AYAYA .

- Description: When the router received the SIP packets which's record-route and contact head field the Transfer Protocol were inconsistent, because the router selected the error Transfer Protocol the voice call failed。

RTD57811

- First found in CMW520-R2207P02
- Condition: The Dialer interface of the router set chap authentication for call-in connection.
- Description: The dialer connection can't establish.

RTD58221

- First found in CMW520-R2207
- Condition: Execute the command of "display ip flow-ordering statistic internal" at the router.
- Description: The router rebooted abnormally.

# Resolved problems in CMW520-R2207P34

RTD57852

- First found in CMW520-R2207P08
- Condition: The router started RIP BFD function.
- Description: After the BFD session at the router was DOWN, the router would delete correlative RIP routes, but the router still sent the RIP packets from the interface. If the interface was broken down in the one direction, another end could still received the rip packets.

RTD57785

- First found in CMW520-E2206
- Condition: The router worked with some SIP SERVER, and established voice calls.
- Description: If the router received the SIP messages which the contact filed of was included the maddr parameter, the voice call from the router was unsuccessful.

RTD57105

- First found in CMW520-R2207P08
- Condition: The MSR30 router has 2 x 512M memories.
- Description: The router reboots itself randomly.

# Resolved problems in CMW520-R2207P33

RTD57709

- First found in CMW520-R2207
- Condition: None.
- Description: The fax function couldn't be started at the router.

# Resolved problems in CMW520-R2207P23

RTD57286

- First found in CMW520-R2207
- Condition: The router doesn't receive connect information from 3G modem.
- Description: Occasionally the router can't recover from PPP state-machine and can't dialup 3G-link successfully.

RTD57514

- First found in CMW520-R2207
- Condition: 3G network was HSPA+.
- Description: The 3G interface of the router would be UP and DOWN.

RTD57364

- First found in CMW520-E2206
- Condition: None.
- Description: The fax function couldn't be started at the router.

RTD57365

- First found in CMW520-E2206
- Condition: The router established the SIP connection with other equipment.
- Description: Because the SDP's fmtp and rtpmap of the SIP packet negotiated by error, the compression selected was wrong.

RTD57500

- First found in CMW520-E2206
- Condition: MPLS L3VPN, inter-AS option B, a route advertising to ASBR through different VPN-instance and the route is flapping.
- Description: The packet which matching this route can't be transmitted.

# Resolved problems in CMW520-R2207P14

RTD56973

- First found in CMW520-R2207
- Condition: 3G network status was unstable, little the network was no service.
- Description: The 3G interface would be UP and DOWN because 3G network was unstable.

RTD56986

- First found in CMW520-R2207
- Condition: The router received the SIP INVITE message without a=T38MaxBitRate filed to transfer T.38.
- Description: The router would turn off the FAX function, and brought on that the FAX failed.

RTD56520

- First found in CMW520-R2207
- Condition: Configuring RIP BFD at the router, the link was uni-direction and the router could receive the RIP packets.
- Description: Even though the RIP BFD session was down, the RIP routes were updated.

RTD56390

- First found in CMW520-R2207
- Condition: The router acted as LNS, and LAC sent the ICCN packets without Proxy auth attribute.
- Description: The router couldn't get the Calling number and Called Number attribute from LAC.

RTD56145

- First found in CMW520-R2207
- Condition: The router acted as LNS, and LAC requested the L2TP packets received with offset field.
- Description: Because the router didn't take offset filed in the L2TP packets, the L2TP connection couldn't establish.

# Resolved problems in CMW520-R2207P02

RTD56119

- First found-in CMW520-R2207

- Condition: If change the DVPN tunnel-protocol when there is IP traffic going out of the tunnel.
- Description: The router will reboot possibly.

RTD56062

- First found-in CMW520-R2207
- Condition: Apply two or more IPSec policy groups to a virtual interface on the web interface, like interface tunnel.
- Description: The IPSec policy groups cannot be modified successfully if the virtual interface is deleted first.

RTD56060

- First found in CMW520-R2207
- Condition: The router received the SIP packet of "200 OK" without "a=silenceSupp:off".
- Description: The router made mistake when negotiating about the codec, it resulted in that the FAX failed.

RTD56106

- First found in CMW520-R2207
- Condition: The packets were identified by DAR after the packets were transmitted through L2TP tunnel.
- Description: The DAR function was abnormal and couldn't identify the packets correctly.

RTD55818

- First found in CMW520-R2207
- Condition: The E1POS interface worked with ISDN signal, and established the ISDN connection with ALCATEL PBX.
- Description: The E1 POS calls failed.

RTD56103

- First found in CMW520-R2207
- Condition: The AR46 or AR28 router worked as RTA relay.
- Description: The A-MSR router as RTA client couldn't establish connection with RTA relay.

# Resolved Problems in CMW520-R2207

RTD54811

- First found in CMW520-R2105P38

- Condition: When using UDP as the SIP transport protocol, If the Packet is huge, the A-MSR cannot re-build the SIP fragment messages.
- Description: The instant message cannot be relaid.

RTD54836

- First found in CMW520-R2105P38
- Condition: When configure the UDP as the SIP transport protocol, If the Packet is larger than MTU-200, the transport protocol will automatically change to TCP, but if the destination does not support TCP, the transport protocol cannot change back to UDP.
- Description: The call cannot be established.

# Resolved Problems in CMW520-R2105P38

RTD55551

- First found in CMW520-R2105P35
- Condition: There were four SIC-BU cards inserted into the router.
- Description: All isdn calls at the four SIC-BU cards couldn't be established successfully at the same time.

RTD55454

- First found in CMW520-R2105P31
- Condition: The router transmitted IPSEC data with perfect forward secrecy function.
- Description: After period of time, IPSEC data would be intermitted.

RTD55494

- First found in CMW520-R2105P31
- Condition: Run the arp fixup command and reboot the router.
- Description: The static arp items are not buildrun after the arp fixup command, so the static arp items will be lost after the device reboot.

# Resolved Problems in CMW520-R2105P36

RTD54196

- First found in CMW520-R2105P02
- Condition: Set x25 bridge map at the interface of the router.
- Description: Even if there were several sub-interfaces at the main-interface, only one x.121 address can be set to map x25 bridge.

RTD54728

- First found in CMW520-R2105P02

- Condition: The source port of mirror-group was MP's virtual-template interface.
- Description: After mirroring the packets for a while, the memory of the router leaked.

RTD54669

- First found in CMW520-R2105P02
- Condition: The G.SHDSL interface of the A-MSR 20-13 was set to 2-wire mode.
- Description: The G.SHDSL interface still negotiated as 4-wire.

# Resolved Problems in CMW520-R2105P35

RTD53977

- First found in CMW520-E2103P04
- Condition: The FR traffic shaping function was enabled at the FR interface, and the CIR of the DLCI was equal to the bandwidth of the interface, the QOS queues were set at the DLCI.
- Description: There were some lost packets at the high PRI queue even if the high priority packets didn't exceed the bandwidth assigned.

# Resolved Problems in CMW520-R2105P31

RTD54152

- First found in CMW520-E2103P04
- Condition: Configure some static ARP entries at the router.
- Description: If the ARP entries updated, the sequence of static ARP entries saved changed.

# Resolved Problems in CMW520-R2105P26

RTD54042

- First found in CMW520-E2103P04
- Condition: Execute the command "save" to save the configuration file at the router, at the same time put the configuration file to the router using TFTP.
- Description: After doing the two operations simultaneity period of time, the router's configuration file lost.

RTD53983

- First found in CMW520-E2103P04
- Condition: Certain interface of the router was bound to the VPN-instance, and was enabled the NAT function.

- Description: The packets transmitted by the interface can't be translated correctly.

RTD53976

- First found in CMW520-E2103P04
- Condition: The two routers established the DLSw peer, and transmitted the packets between the IBM mainframe and SNA host.
- Description: If defining several PU facilities using the same MAC address, the router only could establish virtual circuit for one PU facility.

RTD53848

- First found in CMW520-E2103P04
- Condition: The router acts as LNS established the L2TP connection with other equipment.
- Description: Even though the L2TP client was asynchronous PPP, the router still sent the SLI control packets with ACCM option, and sometime this should bring on that the L2TP connection negotiated unsuccessfully.

RTD53886

- First found in CMW520-R2105P02
- Condition: The FIC/MIM-G.SHDSL cards were inserted into the router, and the G.SHDSL interface established the connection with the Ericsson EDA u2530 DSLAM.
- Description: Ping 900 bytes to 1500 bytes packets from the G.SHDSL interface, and there were lots of packet lost.

# Resolved Problems in CMW520-R2105P22

RTD53762

- First found in CMW520-R2105P02
- Condition: The router acted as SIP voice gateway.
- Description: After running for period of time, the router couldn't establish SIP voice call successfully.

RTD53423

- First found in CMW520-R2105P02
- Condition: The time zone or the summer-time was set at the router, and the router acted as NQA server or client inter-operated with the other equipment.
- Description: The NQA jitter test result was incorrect.

RTD53153

- First found in CMW520-R2105P02
- Condition: NAT function was enabled at the router.

- Description: The Windows PPTP connection couldn't be established successfully, after the PPTP packets were transmitted by the router.

RTD53779

- First found in CMW520-R2105P02
- Condition: None.
- Description: When the signal of VT1 interface is R2, Digital E&M, or LGS, only the timeslot 1-23 can be set.

# Resolved Problems in CMW520-R2105P12

RTD53005

- First found in CMW520-R2105P02
- Condition: The local Portal server was enabled at the router.
- Description: After the user succeeded to login through the local Portal server, the router rebooted exceptionally.

RTD52942

- First found in CMW520-R2105P02
- Condition: Set the NAT server at the router.
- Description: Because NAT ALG transition at the router made mistakes, the H323 call from public network to private network failed in the uni-direction.

RTD53154

- First found in CMW520-R2105P06
- Condition: There were many OSPF neighbors be established at the router.
- Description: Because the OSFP MD5 authentication Sequence could reach to the maximum and overturn at the short time, the OSPF neighbor relationships broke down and re-established.

# Resolved Problems in CMW520-R2105P06

RTD51595

- First found in CMW520-R2104P02
- Condition: When configuration the interface of virtual-template as the output-interface of static route.
- Description: The packets can't be forwarded m.

RTD52249

- First found in CMW520-R2104P02

- Condition: None
- Description: The key of HWTACACS can't more than 96 characters.

RTD52822

- First found in CMW520-E2103P04
- Condition: The Virtual-template interface of the router connected a point-to-point network, and the Virtual-template interface was an output interface of a static route.
- Description: The packets matched up the static route can't be transmitted by the Virtual-template interface, and the static route to Virtual-template was invalid.

RTD52279

- First found in CMW520-R2104P02
- Condition: Run the POS APP function at the AUX interface of the router.
- Description: The POS connections to the AUX interface failed.

RTD52833

- First found in CMW520-R2105P02
- Condition: The VOIP function was enabled at the router, and the ISDN SETUP message from the PBX didn't contain the caller name, instead the caller name was included at the following Facility message.
- Description: The caller name couldn't be displayed at the called.

# Resolved Problems in CMW520-R2105P02

RTD51702

- First found in CMW520-R2104P02
- Condition: Plug the USB 3G Modem in and reboot the router with empty configuration.
- Description: Then the router can't recognize the USB 3G Modem.

RTD51603

- First found in CMW520-R2104P02
- Condition: When configuration the command of "nat outbound" on the interface.
- Description: The router will be crash when send packets of ICMP unreachable.

RTD51986

- First found in CMW520-R2104P02
- Condition: None
- Description: The A-MSR 30-16 didn't support the DMC function, and there is any command of DMC at the A-MSR 30-16.

RTD52094

- First found in CMW520-R2104P02
- Condition: None.
- Description: The NAS-IP can't be set to the IP address ended with 255 at the router.

RTD51965

- First found in CMW520-R2104P02
- Condition: Start the NAT function at the router.
- Description: When the router received the especial DNS reverse-query packets, the router did the NAT translation, then the router rebooted abnormally.

RTD51868

- First found in CMW520-R2104P02
- Condition: The router worked as voice gateway, and the router ran the R2 signal with the PBX E1.
- Description: If the PBX's E1 took a long time to responding to the router, the H323 timer of the router will be timeout, then the voice all can't be established successfully.

RTD51715

- First found in CMW520-R2104P02
- Condition: Enable the ASPF function at the router.
- Description: The Linux FTP client couldn't visit the Serv-U ftp server transmitted by the router.

RTD51666

- First found in CMW520-R2104P02
- Condition: None.
- Description: Because the ADSL Modem XAVI model x7822m should send the ARP packets with 0000-0000-0000 MAC, the router can't established the connection with this ADSL Modem.

RTD51593

- First found in CMW520-R2104P02
- Condition: There is a loopback interface and another interface which's ip addres is the same IP network segment with the loopback interface.
- Description: If the ip address of the loopback interface is set before the ip address of another interface is set, the router can't telnet the ip address of its loopback interface successfully.

RTD51592

- First found in CMW520-R2104P02

- Condition: The router ran multilink PPP linked with some equipment.
- Description: Because the router responded NAK packet when it received the MRRU more than 0x4000, the router can't establish the connection with some equipment.

RTD51760

- First found in CMW520-E2103P04
- Condition: None.
- Description: On the router direct route and LDP does not accept the label from the direct peer.

# Resolved Problems in CMW520-R2105

RTD51163

- First found in CMW520-R2104P02
- Condition: When receiving a SIP message, if its SDP rtpmap and fmtp are not in order, the codec negotiation may be failed.
- Description: Codec negotiation may be failed, and the call can not be setup.

RTD51162

- First found in CMW520-R2104P02
- Condition: When neotiating T.38 in SIP Messages, after the negotiation, t.38 packets were not marked with DSCP.
- Description: Because T.38 packets were not marked with DSCP, QoS policy may be mismatch and unuseful.

# Related documentation

## New feature documentation

None.

## Documentation set

Table 15 Documentation set

| Document title | Version |
|---|---|
| About the HP A-MSR Command References | 6PW100 |
| About the HP A-MSR Configuration Guides | 6PW100 |
| HP A-MSR Router Series ACL and QoS Command Reference | 6PW100 |

| Document title | Version |
|---|---|
| HP A-MSR Router Series ACL and QoS Configuration Guide | 6PW100 |
| HP A-MSR Router Series Fundamentals Command Reference | 6PW100 |
| HP A-MSR Router Series Fundamentals Configuration Guide | 6PW100 |
| HP A-MSR Router Series High Availability Command Reference | 6PW100 |
| HP A-MSR Router Series High Availability Configuration Guide | 6PW100 |
| HP A-MSR Router Series IP Multicast Command Reference | 6PW100 |
| HP A-MSR Router Series IP Multicast Configuration Guide | 6PW100 |
| HP A-MSR Router Series IPX Command Reference | 6PW100 |
| HP A-MSR Router Series IPX Configuration Guide | 6PW100 |
| HP A-MSR Router Series Interface Command Reference | 6PW100 |
| HP A-MSR Router Series Interface Configuration Guide | 6PW100 |
| HP A-MSR Router Series Interface Modules Guide | 6PW100 |
| HP A-MSR Router Series Layer 2 - LAN Switching Command Reference | 6PW100 |
| HP A-MSR Router Series Layer 2 - LAN Switching Configuration Guide | 6PW100 |
| HP A-MSR Router Series Layer 2 - WAN Command Reference | 6PW100 |
| HP A-MSR Router Series Layer 2 - WAN Configuration Guide | 6PW100 |
| HP A-MSR Router Series Layer 3 - IP Routing Command Reference | 6PW100 |
| HP A-MSR Router Series Layer 3 - IP Routing Configuration Guide | 6PW100 |
| HP A-MSR Router Series Layer 3 - IP Services Command Reference | 6PW100 |
| HP A-MSR Router Series Layer 3 - IP Services Configuration Guide | 6PW100 |
| HP A-MSR Router Series MPLS Command Reference | 6PW100 |
| HP A-MSR Router Series MPLS Configuration Guide | 6PW100 |
| HP A-MSR Router Series Network Management and Monitoring Command Reference | 6PW100 |
| HP A-MSR Router Series Network Management and Monitoring Configuration Guide | 6PW100 |
| HP A-MSR Router Series OAA Command Reference | 6PW100 |
| HP A-MSR Router Series OAA Configuration Guide | 6PW100 |
| HP A-MSR Router Series Security Command Reference | 6PW100 |
| HP A-MSR Router Series Security Configuration Guide | 6PW100 |
| HP A-MSR Router Series Terminal Access Command Reference | 6PW100 |
| HP A-MSR Router Series Terminal Access Configuration Guide | 6PW100 |
| HP A-MSR Router Series Voice Command Reference | 6PW100 |
| HP A-MSR Router Series Voice Configuration Guide | 6PW100 |
| HP A-MSR Router Series WLAN Command Reference | 6PW100 |
| HP A-MSR Router Series WLAN Configuration Guide | 6PW100 |
| HP A-MSR Router Series Web-Based Configuration Guide | 6PW100 |

# Obtaining documentation

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

# Software upgrading

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

# System software file types

System software images are in .bin format (for example, main.bin) and run at startup. Yon can set a system software image as a main, backup, or secure image.

At startup, the router always attempts to boot first with the main system software image. If the attempt fails, for example, because the image file is corrupted, the router tries to boot with the backup system software image. If the attempt still fails, the router tries to boot with the secure system software image. If all attempts fail, the router displays a failure message.

# Upgrade methods

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

| Upgrade method | Remarks |
|---|---|
| Upgrading from the CLI | You must reboot the router to complete the upgrade.<br>This method can interrupt ongoing network services. |
| Upgrading 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:

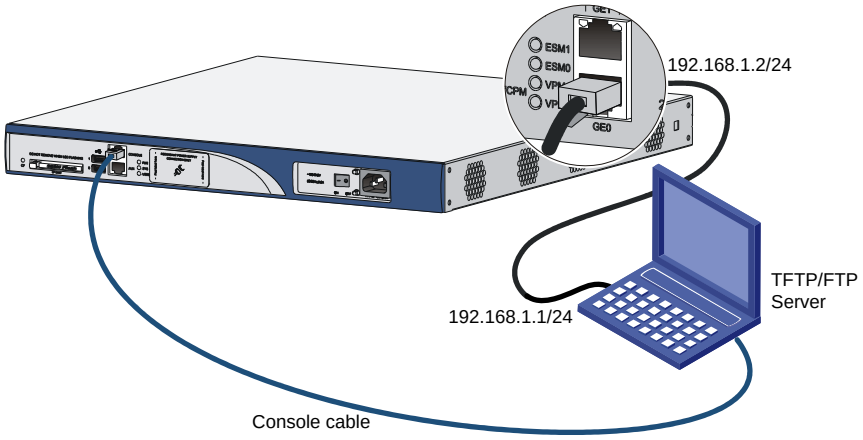
- Set up the upgrade environment as shown in Table 16 5.
- Configure routes to make sure that the router and the file server can reach each other.
- Run a TFTP or FTP server on the file server.

- Log in to the CLI of the router through the console port.
- Copy the upgrade file to the file server and correctly set the working directory on the TFTP or FTP server.
- Make sure that the upgrade has minimal impact on the network services. During the upgrade, the router cannot provide any services.

IMPORTANT:

- In the BootWare menu, if you choose to download files over Ethernet, the Ethernet port must be ETH0 on an A-MSR900, A-MSR20-1X, or A-MSR20 router, and must be GE0 on an A-MSR30 or A-MSR50 router.

Figure 1 Set up the upgrade environment




# 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.

## Using TFTP to upgrade software

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

### Backing up the running system software image and configuration file

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

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

```
 Configuration is saved to device successfully.
<Sysname>
```

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.

```
<Sysname> dir
Directory of cfa0:/

   0     drw-         -  Jun 28 2011 14:41:16   logfile
   1     drw-         -  Jun 28 2011 14:42:56   domain1
   2     -rw-     16256  Jun 28 2011 14:43:40   p2p_default.mtd
   3     -rw-      1694  Jun 28 2011 14:47:12   startup.cfg
   4     -rw-      3432  Jun 28 2011 14:47:10   system.xml
   5     -rw-  23861744  Jun 28 2011 14:37:46   main.bin

252328 KB total (227856 KB free)

File system type of cfa0: FAT16

<Sysname>
```

This example uses the default system software image file name main.bin and the default configuration file name startup.cfg.

3. Perform the tftp put command in user view to upload the main.bin file to the TFTP server.

```
<Sysname> tftp 192.168.1.1 put main.bin

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP: 23861744 bytes sent in 70 second(s).
  File uploaded successfully.

<Sysname>
```

4. Perform the tftp put command in user view to upload the startup.cfg file to the TFTP server.

```
<Sysname> tftp 192.168.1.1 put startup.cfg
  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:     1694 bytes sent in 0 second(s).
  File uploaded successfully.

<Sysname>
```

## Upgrading the system software

1. Perform the tftp get command in user view to download the system software image file, for example, A_MSR30-CMW520-R2207-SI.BIN to the CF card on the router.

```
<Sysname> tftp 192.168.1.1 get A_MSR30-CMW520-R2207-SI.BIN
```

```
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP: 23861744 bytes received in 70 second(s)
  File downloaded successfully.

<Sysname>
```

2. Perform the boot-loader command in user view to load the file A_MSR30-CMW520-R2207-SI.BIN and specify the file as the main image file at the next reboot.

```
<Sysname> boot-loader file a_msr30-cmw520-r2207-si.bin main
  This command will set the boot file. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot
0!
<Sysname>
```

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

```
<Sysname> display boot-loader
 The boot file used at this reboot:cfa0:/main.bin attribute: main
 The boot file used at the next reboot:cfa0:/a_msr30-cmw520-r2207-si.bin attribute:
main
 Failed to get the backup boot file used at the next reboot!
 Failed to get the secure boot file used at the next reboot!
<Sysname>
```

4. Perform the reboot command in user view to reboot the router.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
#Jun 28 16:17:22:368 2011 HP DEVM/1/REBOOT:
 Reboot device by command.
%Jun 28 16:17:22:368 2011 HP DEVM/5/SYSTEM_REBOOT: System is rebooting now.
 Now rebooting, please wait...
<Sysname>
System is starting...
```

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

```
<Sysname>display version
HP Comware Platform Software
Comware Software, Version 5.20, Release 2207, Standard
Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
HP A-MSR30-20 uptime is 0 week, 0 day, 0 hour, 3 minutes
Last reboot 2011/06/28 16:19:05
System returned to ROM By <Reboot> Command.

CPU type: FREESCALE MPC8349 533MHz
```

```
256M bytes DDR SDRAM Memory
4M bytes Flash Memory
Pcb               Version:  3.0
Logic             Version:  2.0
Basic    BootROM  Version:  3.12
Extended BootROM  Version:  3.13
[SLOT  0]CON                     (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]AUX                     (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]GE0/0                   (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]GE0/1                   (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]CELLULAR0/0             (Hardware)3.0    (Driver)1.0,    (Cpld)2.0

<Sysname>
```

# Using FTP to upgrade software

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

## Backing up the running system software image and configuration file

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

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

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.

```
<Sysname> dir
Directory of cfa0:/

   0     drw-         -  Jun 28 2011 14:41:16   logfile
   1     drw-         -  Jun 28 2011 14:42:56   domain1
   2     -rw-     16256  Jun 28 2011 14:43:40   p2p_default.mtd
   3     -rw-      1694  Jun 28 2011 14:47:12   startup.cfg
   4     -rw-      3432  Jun 28 2011 14:47:10   system.xml
   5     -rw-  23861744  Jun 28 2011 14:37:46   main.bin

252328 KB total (227856 KB free)

File system type of cfa0: FAT16

<Sysname>
```

This example uses the default system software image file name main.bin and the default configuration file name startup.cfg.

3. Perform the ftp command in user view to access the FTP server.

```
<Sysname> ftp 192.168.1.1
Trying 192.168.1.1 ...
Press CTRL+K to abort
Connected to 192.168.1.1.
220 3Com 3CDaemon FTP Server Version 2.0
User(192.168.1.100:(none)):user001
331 User name ok, need password
Password:
230 User logged in
```

4. Perform the put command in FTP client view to upload the main.bin file to the FTP server.

```
[ftp] put main.bin
227 Entering passive mode (192,168,1,1,7,210)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 23861744 byte(s) sent in 21.363 second(s), 1116.00Kbyte(s)/sec.

[ftp]
```

5. Perform the put command in FTP client view to upload the startup.cfg file to the FTP server.

```
[ftp] put startup.cfg
227 Entering passive mode (192,168,1,1,7,177)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 1677 byte(s) sent in 0.142 second(s), 11.00Kbyte(s)/sec.

[ftp]
```

## Upgrading the system software

1. Perform the get command in FTP client view to download the system software image file A_MSR30-CMW520-R2207-SI.BIN to the CF card on the router.

```
[ftp] get a_msr20-cmw520-r2207-si.bin

227 Entering passive mode (192,168,1,1,7,225)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 23861744 byte(s) received in 30.907 second(s), 772.00K byte(s)/sec.

[ftp]
```

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

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

```
<Sysname>
```

3. Perform the boot-loader command in user view to load the file A_MSR30-CMW520-R2207-SI.BIN and specify the file as the main image file at the next reboot.

```
<Sysname> boot-loader file a_msr30-cmw520-r2207-si.bin main
  This command will set the boot file. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot
0!
<Sysname>
```

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

```
<Sysname> display boot-loader
 The boot file used at this reboot:cfa0:/main.bin attribute: main
 The boot file used at the next reboot:cfa0:/a_msr30-cmw520-r2207-si.bin attribute:
main
 Failed to get the backup boot file used at the next reboot!
 Failed to get the secure boot file used at the next reboot!
<Sysname>
```

5. Perform the reboot command in user view to reboot the router.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
#Jun 28 16:17:22:368 2011 HP DEVM/1/REBOOT:
 Reboot device by command.
%Jun 28 16:17:22:368 2011 HP DEVM/5/SYSTEM_REBOOT: System is rebooting now.
 Now rebooting, please wait...
<Sysname>
System is starting...
```

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

```
<Sysname>display version
HP Comware Platform Software
Comware Software, Version 5.20, Release 2207, Standard
Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
HP A-MSR30-20 uptime is 0 week, 0 day, 0 hour, 3 minutes
Last reboot 2011/06/28 16:19:05
System returned to ROM By <Reboot> Command.

CPU type: FREESCALE MPC8349 533MHz
256M bytes DDR SDRAM Memory
4M bytes Flash Memory
Pcb               Version:  3.0
Logic             Version:  2.0
Basic    BootROM  Version:  3.12
```

```
Extended BootROM  Version:  3.13
[SLOT  0]CON                        (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]AUX                        (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]GE0/0                      (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]GE0/1                      (Hardware)3.0    (Driver)1.0,    (Cpld)2.0
[SLOT  0]CELLULAR0/0                (Hardware)3.0    (Driver)1.0,    (Cpld)2.0

<Sysname>
```

# 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

TIP:

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

## Accessing the BootWare menu

1. Power on the router (for example, an HP A-MSR30-20 router), and you can see the following information:

```
System is starting...

Do you want to check SDRAM? [Y/N]

Booting Normal Extend BootWare........

The Extend BootWare is self-decompressing.....................

Done!

********************************************************************************

*                                                                              *

*                HP A-MSR30-20  BootWare, Version 3.12                         *

*                                                                              *

********************************************************************************

Copyright (c) 2004-2010 Hewlett-Packard Development Company, L.P.

Compiled Date       : Feb 16 2011

CPU Type            : MPC8349E

CPU L1 Cache        : 32KB
```

```
CPU Clock Speed     : 533MHz

Memory Type         : DDR SDRAM

Memory Size         : 256MB

Memory Speed        : 264MHz

BootWare Size       : 4096KB

Flash Size          : 4MB

cfa0 Size           : 256MB

CPLD Version        : 2.0

PCB Version         : 3.0



BootWare Validating...

Press Ctrl+B to enter extended boot menu...
```

2. Press Ctrl + B at the prompt.

```
Please input BootWare password:
```

3. Enter the BootWare password at the prompt to access the BootWare menu.

   By default, no password is required.

   If three password attempts are failed, the system reboots.

```
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> Modify BootWare Password                                            |

|<6> Skip Current System Configuration                                   |

|<7> BootWare Operation Menu                                             |

|<8> Clear Super Password                                                |

|<9> Storage Device Operation                                            |
```

```
|<0> Reboot                                                                |

==========================================================================

Enter your choice(0-9)::
```

Table 16 BootWare menu options

| Item | Description |
|---|---|
| <1> Boot System | Boot the system software image. |
| <2> Enter Serial SubMenu | Access the Serial submenu (see Table 19 ) for upgrading system software through the console port or changing the serial port settings. |
| <3> Enter Ethernet SubMenu | Access the Ethernet submenu (see Table 17 ) for upgrading system software through an Ethernet port or changing Ethernet settings. |
| <4> File Control | Access the File Control submenu (see Table 20 ) to retrieve and manage the files stored on the router. |
| <5> Modify BootWare Password | Modify the BootWare password. For security, HP recommends you set a BootWare password the first time you access the router. |
| <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. HP does not recommend upgrading BootWare separately. This document does not cover using the BootWare Operation menu. |
| <8> Clear Super Password | Clear all super passwords used for switching to higher user privilege levels.<br>By default, no super password is required for switching to a higher user privilege level. |
| <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.

```
=========================<Enter Ethernet SubMenu>=========================
|Note:the operating device is cfa0                                        |
|<1> Download Application Program To SDRAM And Run                        |
|<2> Update Main Application File                                         |
|<3> Update Backup Application File                                       |
|<4> Update Secure Application File                                       |
|<5> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
|<Ensure The Parameter Be Modified Before Downloading!>                   |
==========================================================================
Enter your choice(0-5):
```

Table 17 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 Application File | Upgrade the main system software image. |
| | <3> Update Backup Application File | Upgrade the backup system software image. |
| | <4> Update Secure Application File | Upgrade the secure system software image. |
| | <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) :tftp
Load File Name         :main.bin
                       :
Target File Name       :main.bin
                       :
Server IP Address      :192.168.1.1
Local IP Address       :192.168.1.253
Gateway IP Address     :0.0.0.0
FTP User Name          :user
```

```
FTP User Password      :password
```

Table 18 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. |
| 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!
31911744 bytes downloaded!
Updating File flash:/main.bin.....................................................
.....................................................Done!
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is flash                                         |
|<1> Download Application Program To SDRAM And Run                          |
|<2> Update Main Application File                                           |
|<3> Update Backup Application File                                         |
|<4> Update Secure Application File                                         |
|<5> Modify Ethernet Parameter                                              |
|<0> Exit To Main Menu                                                      |
```

```
|<Ensure The Parameter Be Modified Before Downloading!>                    |
==========================================================================
Enter your choice(0-5):
```

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

# 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 Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
==========================================================================
Enter your choice(0-5):
```

Table 19 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 Application File | Upgrade the main system software image. |
| <3> Update Backup Application File | Upgrade the backup system software image. |
| <4> Update Secure Application File | Upgrade the secure system software image. |
| <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):5
```

The following messages appear:

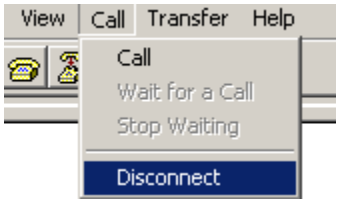
```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

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

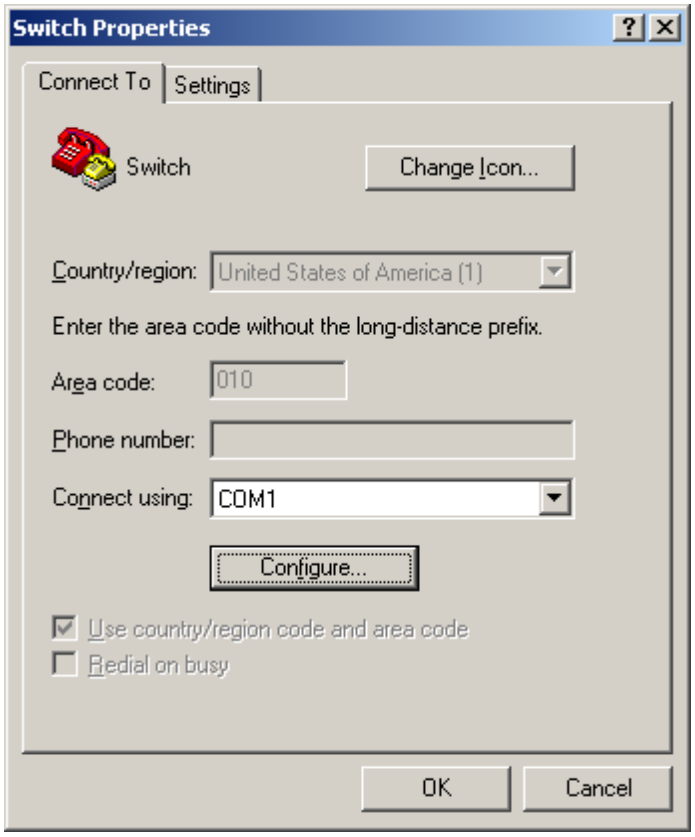



NOTE:

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

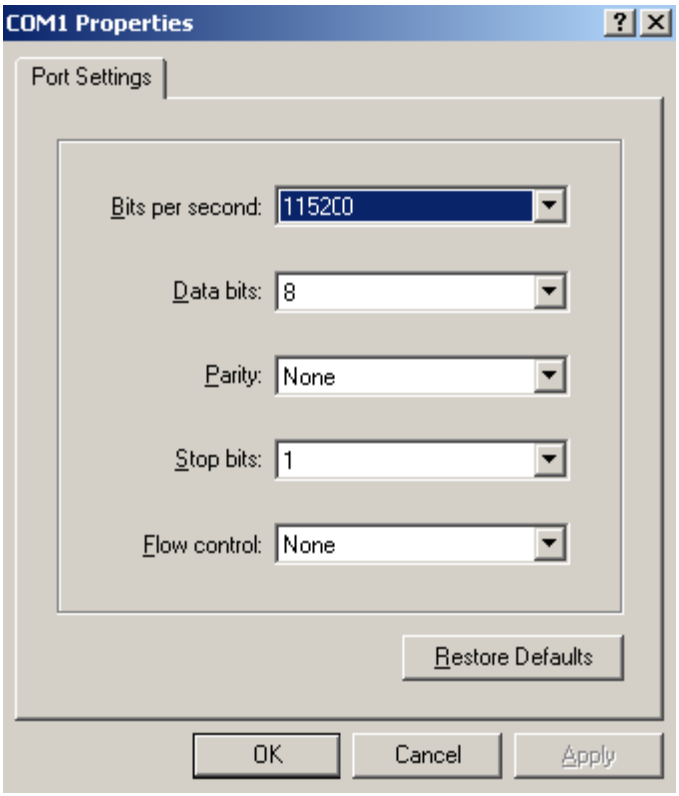
4. Select File > Properties, and in the Properties dialog box, click Configure.

Figure 3 Properties dialog box



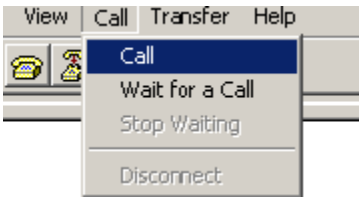

5. Select 115200 from the Bits per second list and click OK.

Figure 4 Modify the baud rate




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.

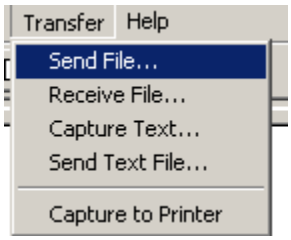
```
============================<Enter Serial SubMenu>============================
|Note:the operating device is flash                                         |
|<1> Download Application Program To SDRAM And Run                          |
|<2> Update Main Application File                            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

9. Select an option from options 2 to 4 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
```

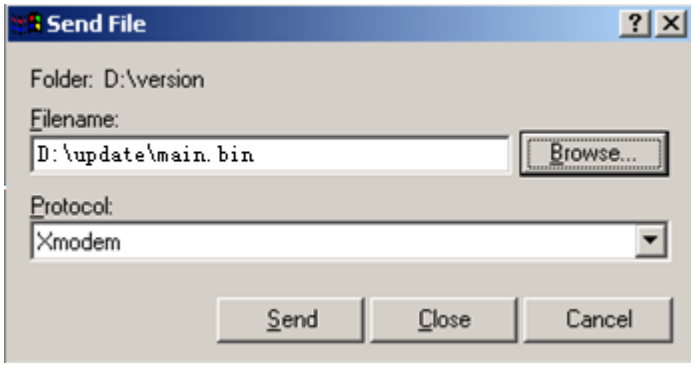
10. Select Transfer > Send File in the HyperTerminal window.

Figure 6 Transfer menu



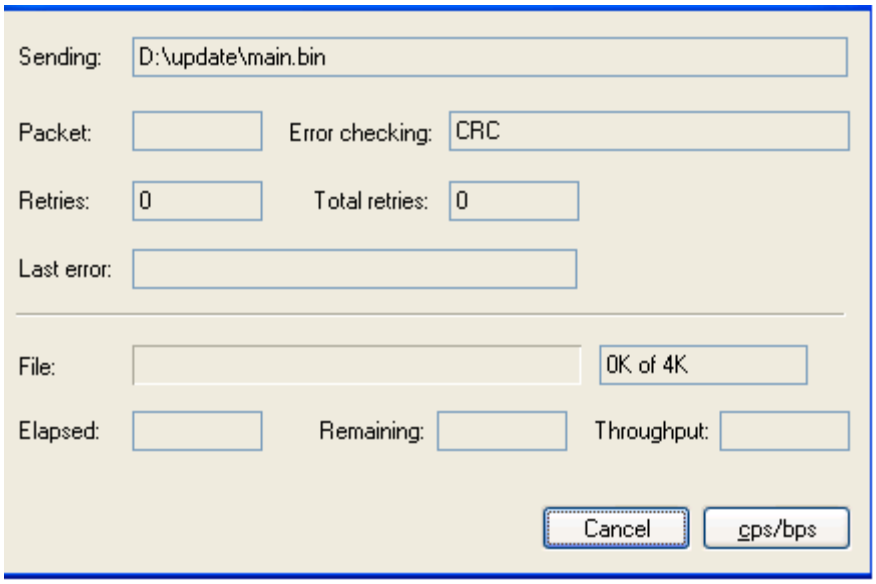

11. In the dialog box that appears, click Browse to select the source file, and select Xmodem from the Protocol list.

Figure 7 File transmission dialog box




12. Click Send. The following dialog box appears:

Figure 8 File transfer progress




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!
31911808 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 Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
==============================================================================
Enter your choice(0-5):
```

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 Application File type                                       |
|<3> Set Configuration File type                                     |
|<4> Delete File                                                     |
|<0> Exit To Main Menu                                               |
======================================================================
Enter your choice(0-4):
```

Table 20 File Control submenu options

| Item | Description |
|---|---|
| <1> Display All File | Display all files. |
| <2> Set Application File type | Change the type of a system software image. |
| <3> Set Configuration File type | Change the type of a configuration file. |
| <4> Delete File | Delete files. |
| <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 cfa0:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
======================================================================
|NO. Size(B)    Time                 Type    Name                     |
|1   640199     Dec/20/2007 09:53:16 N/A     cfa0:/logfile/logfile.log|
|2   22165484   Dec/20/2007 09:18:10 B+S     cfa0:/update.bin         |
|3   1181       Dec/20/2007 09:42:54 N/A     cfa0:/startup.cfg        |
|4   22165484   Dec/20/2007 09:42:28 M       cfa0:/main.bin           |
======================================================================
```

# Changing the type of a system software image

System software image file attributes include main (M), backup (B), and secure (S). You can store only one main image, one backup image, and one secure image on the router. A system software image can have any combination of the M, B, and S 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.

For example, the file main.bin has the M attribute and the file update.bin has the S attribute. After you assign the M attribute to update.bin, the type of update.bin changes to M+S and the type of main.bin changes to N/A.

NOTE:

You cannot remove or assign the S attribute in the File Control submenu.

To change the type of a system software image:

1. Enter 2 in the File Control submenu.

```
'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
|NO. Size(B)    Time                  Type    Name                            |
|1   22165484   Dec/20/2007 09:18:10 B+S     cfa0:/update.bin                |
|2   22165484   Dec/20/2007 09:42:28 M       cfa0:/main.bin                  |
|0   Exit                                                                    |
================================================================================
Enter file No:
```

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

```
Modify the file attribute:
================================================================================
|<1> +Main                                                                    |
|<2> -Main                                                                    |
|<3> +Backup                                                                  |
|<4> -Backup                                                                  |
|<0> Exit                                                                    |
================================================================================
Enter your choice(0-4):
```

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 4 in the File Control submenu.

```
Deleting the file in cfa0:

 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED

================================================================================

|NO. Size(B)    Time                  Type    Name                            |

|1   640199     Dec/20/2007 09:53:16 N/A     cfa0:/logfile/logfile.log       |

|2   22165484   Dec/20/2007 09:18:10 B+S     cfa0:/update.bin                |

|3   1181       Dec/20/2007 09:42:54 N/A     cfa0:/startup.cfg               |

|4   22165484   Dec/20/2007 09:42:28 M       cfa0:/main.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 cfa0:/backup.bak,Delete it? [Y/N]Y

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

# Handling software upgrade failures

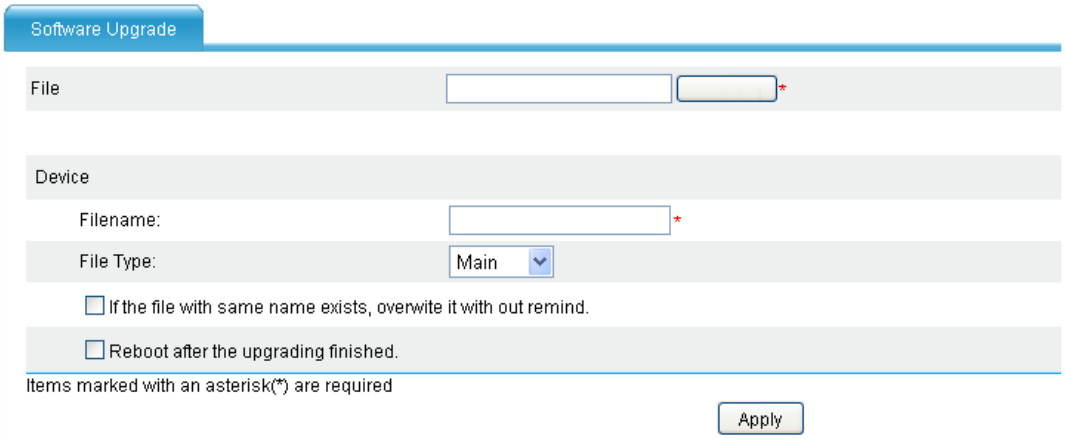
If a software upgrade fails, the system runs the old software version. To handle a software failure:

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.

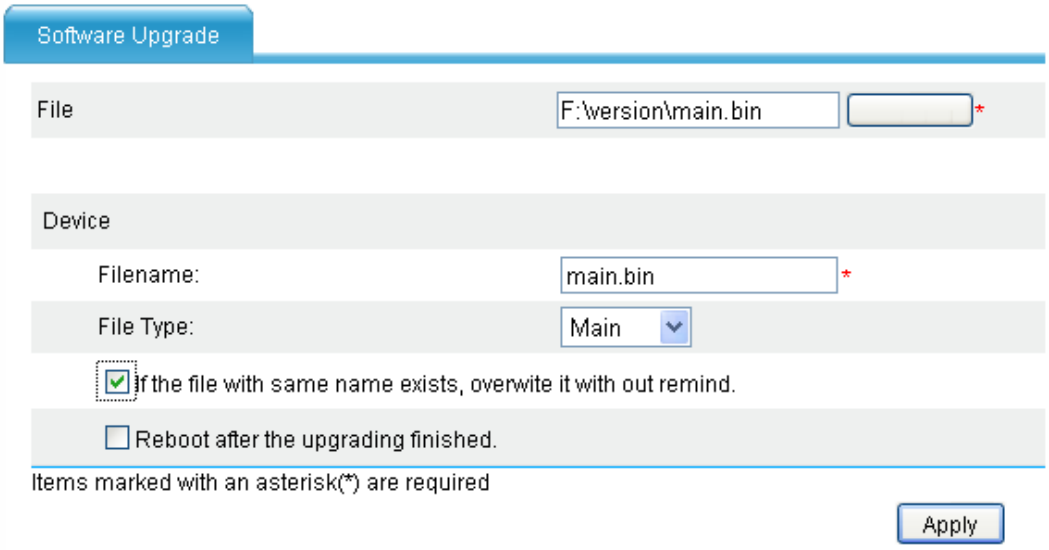
# Software Upgrading Through Web

The device obtains the target application file in the user-defined path through HTTP and has the system upgraded to the target version at the next reboot.

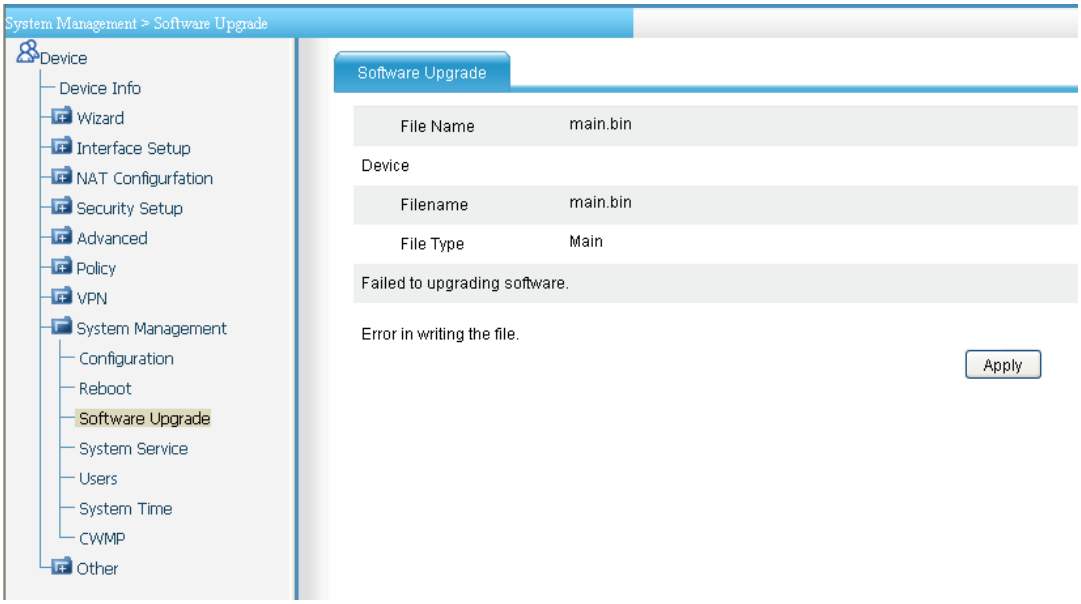
Select **System Management** > **Software Upgrade** from the navigation tree to enter the page as shown below.



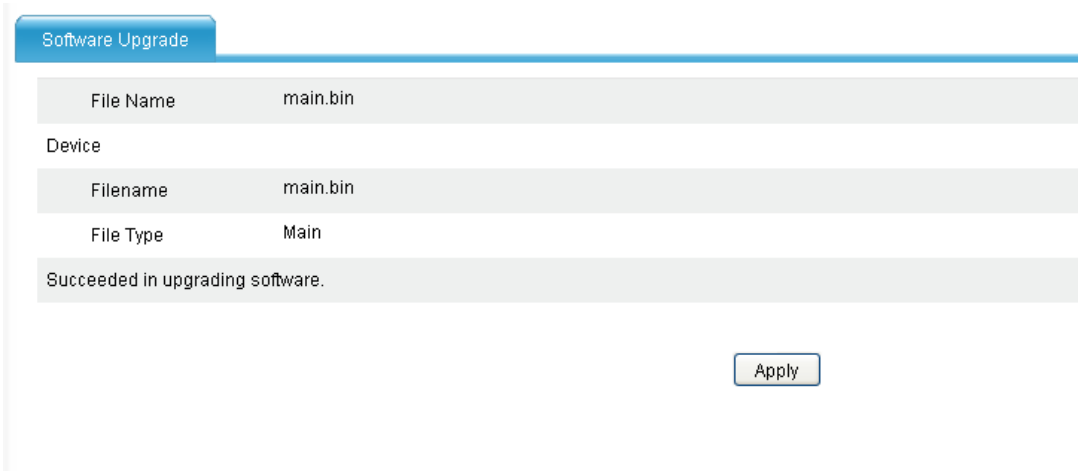

Click **Browse**. On the dialog box displayed, select the target application file in the local path, and specify the name of the application file to be stored on the device. Then select the **If the file with same name exists, overwrite it out remind** check box. Click **Apply** to upgrade the software, as shown in the following figure.



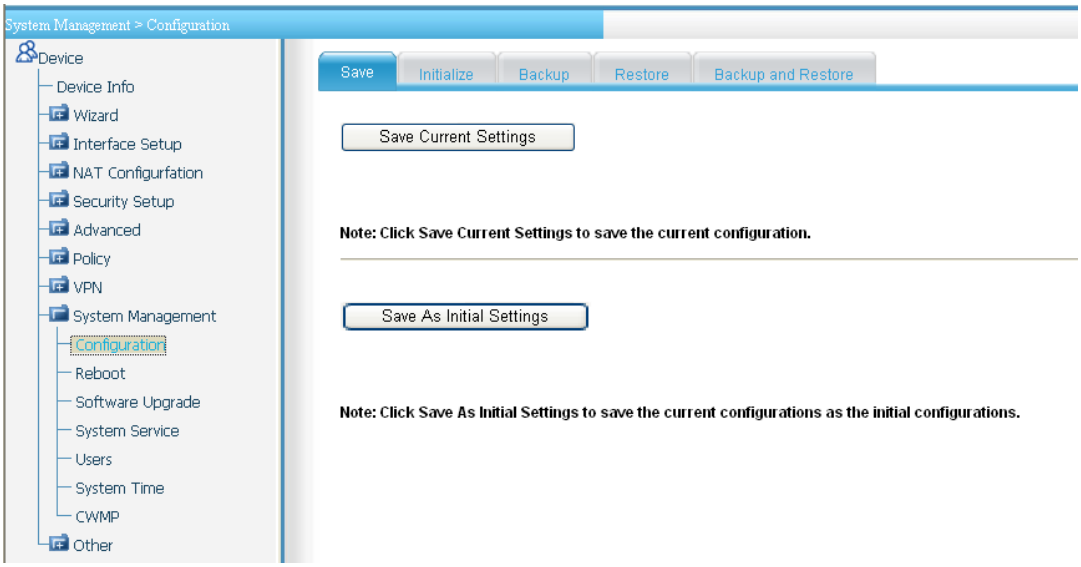

The upgrade process takes about three to five minutes. During this process, ensure that the network connection is normal and do not power off or restart the device.



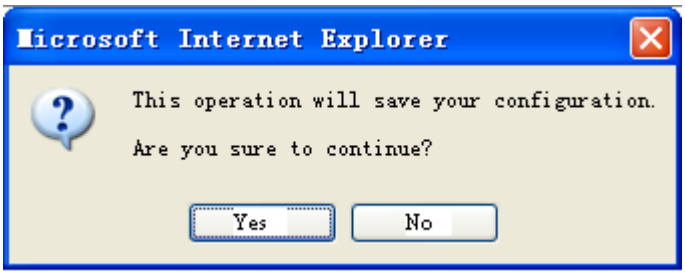

After the upgrade is complete, the system displays the following information and you need to restart the device.




Before restarting the device, follow these steps to save the current system configuration: select **System Management** > **Configuration** from the navigation tree to enter the default **Save** page, and then click **Save Current Settings**, as shown in the following figure.




Click **Yes** in the pop-up dialog box.




After saving the configuration information, select **System Management** > **Reboot** from the navigation tree to enter the page shown below. Click **Apply** to reboot the device.