Abstract: This release notes describes the Switch 4210 R2215P12 release with respect to version information, updating, unresolved problems, and solved problems.

Acronyms:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full spelling</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>BPS</td>
<td>Bit Per Second</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Codepoint Priority</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EPON</td>
<td>Ethernet Passive Optical Network</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GARP</td>
<td>Generic Attribute Registration Protocol</td>
</tr>
<tr>
<td>GVRP</td>
<td>GARP VLAN Registration Protocol</td>
</tr>
<tr>
<td>HGMP</td>
<td>Huawei Group Management Protocol</td>
</tr>
<tr>
<td>HQ</td>
<td>High-Priority Queuing</td>
</tr>
<tr>
<td>HGMP</td>
<td>Huawei Group Management Protocol</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIB</td>
<td>Manage Information Base</td>
</tr>
<tr>
<td>MSTP</td>
<td>Multiple Spanning Tree Protocol</td>
</tr>
<tr>
<td>NDP</td>
<td>Neighbor Discover Protocol</td>
</tr>
<tr>
<td>NTDP</td>
<td>Neighbor Topology Discovery Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full spelling</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>ONU</td>
<td>Optical Network Unit</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RMON</td>
<td>Remote Monitoring</td>
</tr>
<tr>
<td>RSPAN</td>
<td>Remote Switched Port Analyzer</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transfer Control Protocol</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VCT</td>
<td>Virtual Cable Test</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VFS</td>
<td>Virtual File System</td>
</tr>
<tr>
<td>WRR</td>
<td>Weighted Round Robin</td>
</tr>
</tbody>
</table>
# Table of Contents

**Version Information** ................................................................. 6  
Version Number ........................................................................ 6  
Version History ......................................................................... 6  
Hardware and Software Compatibility Matrix ............................. 6  

**Restrictions and Cautions** ......................................................... 7  

**Feature List** ........................................................................... 8  
Hardware Features ..................................................................... 8  
Software Features ...................................................................... 9  

**Version Updates** .................................................................... 11  
Feature Updates ......................................................................... 11  
Command Line Updates ............................................................... 12  
MIB Updates ............................................................................. 13  
Configuration Changes ............................................................... 14  
  Configuration Changes in CMW310-R2215P12 .......................... 14  
  Configuration Changes in CMW310-R2215P11 .......................... 14  
  Configuration Changes in CMW310-R2212P01 .......................... 14  
  Configuration Changes in CMW310-R2212 .............................. 14  

**Open Problems and Workarounds** .......................................... 15  

**List of Resolved Problems** ...................................................... 15  
Resolved Problems in CMW310-R2215P12 .................................. 15  
Resolved Problems in CMW310-R2215P11 .................................. 15  
Resolved Problems in CMW310-R2212P01 .................................. 15  
Resolved Problems in CMW310-R2212 ...................................... 21  

**Related Documentation** ........................................................... 21  

**Software Upgrading** ............................................................... 21  
Remote Upgrading through CLI .................................................. 22  
Boot Menu ................................................................................ 23  
Software Upgrading via Console Port (Xmodem Protocol) ........... 24  
Software Upgrading via Ethernet Interface (FTP/TFTP) .......... 26  
  Using TFTP Through an Ethernet Interface ............................ 26  
  Using FTP Through an Ethernet Interface ............................. 27  

**Appendix** ............................................................................ 27  
Details of Modified CLI Commands in R2215P12 ...................... 28  
bims-server ............................................................................. 28  
dhcp server bims-server ............................................................ 28  
dldp authentication-mode ......................................................... 29  
key (HWTACACS scheme view) ................................................... 30  
key (RADIUS scheme view) ....................................................... 31
local-server nas-ip ........................................................................................................................................... 31
mac-authentication authmode usernameasmacaddress .............................................................................. 32
mac-authentication authpassword .................................................................................................................. 33
ntp-service authentication-keyid .................................................................................................................... 34
password (Remote-ping test group view ) ........................................................................................................ 34
password (local user view) ............................................................................................................................... 35
primary accounting (RADIUS scheme view) .................................................................................................... 36
primary authentication (RADIUS scheme view) .............................................................................................. 36
secondary accounting (RADIUS scheme view) ................................................................................................ 37
secondary authentication (RADIUS scheme view) ............................................................................................ 38
set authentication password ............................................................................................................................. 39
snmp-agent usm-user v3 ...................................................................................................................................... 39
super password .................................................................................................................................................. 41
List of Tables

Table 1 Version history .............................................................................................................................. 6
Table 2 Hardware and software compatibility matrix................................................................................. 6
Table 3 Hardware features (1)................................................................................................................... 8
Table 4 Hardware features (2)................................................................................................................... 8
Table 5 Software features.......................................................................................................................... 9
Table 6 Feature updates........................................................................................................................... 11
Table 7 Command line updates................................................................................................................ 12
Table 8 MIB updates................................................................................................................................. 13
Table 9 Encrypted authentication key length requirements..................................................................... 40
Table 10 Encrypted privacy key length requirements.............................................................................. 40
Version Information

Version Number


Note: To view version information, use the display version command in any view. See Note①.

Version History

Table 1 Version history

<table>
<thead>
<tr>
<th>Version number</th>
<th>Last version</th>
<th>Release Date</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMW310-R2215P12</td>
<td>CMW310-R2215P11</td>
<td>2012-12-17</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2215P11</td>
<td>CMW310-R2212P01</td>
<td>2012-10-19</td>
<td>Usage version</td>
</tr>
<tr>
<td>CMW310-R2212P01</td>
<td>CMW310-R2212</td>
<td>2010-09-10</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212</td>
<td>First release</td>
<td>2009-12-21</td>
<td>None</td>
</tr>
</tbody>
</table>

Hardware and Software Compatibility Matrix

Table 2 Hardware and software compatibility matrix

<table>
<thead>
<tr>
<th>Item</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product family</td>
<td>Switch 4210 series</td>
</tr>
<tr>
<td>Hardware platform</td>
<td>• Switch 4210 9-Port (3CR17331A-91)</td>
</tr>
<tr>
<td></td>
<td>• Switch 4210 18-port (3CR17332A-91)</td>
</tr>
<tr>
<td></td>
<td>• Switch 4210 26-port (3CR17333A-91)</td>
</tr>
<tr>
<td></td>
<td>• Switch 4210 PWR 9-port (3CR17341A-91)</td>
</tr>
<tr>
<td></td>
<td>• Switch 4210 PWR 18-port (3CR17342A-91)</td>
</tr>
<tr>
<td></td>
<td>• Switch 4210 PWR 26-port (3CR17343A-91)</td>
</tr>
<tr>
<td></td>
<td>• Switch 4210 52-port (3CR17334-91)</td>
</tr>
<tr>
<td>Minimum memory requirements</td>
<td>64 MB</td>
</tr>
<tr>
<td>Minimum Flash requirements</td>
<td>8 MB</td>
</tr>
<tr>
<td>Boot ROM version</td>
<td>V610 or higher (You can view the version number with the display version command in any view. Please see Note②)</td>
</tr>
<tr>
<td>Host software</td>
<td>S4210-CMW310-R2215P12-S168.bin</td>
</tr>
<tr>
<td>iMC version</td>
<td>iMC PLAT 5.1 SP1 (E0202P05)</td>
</tr>
<tr>
<td></td>
<td>iMC UAM 5.1 SP1 (E0301P03)</td>
</tr>
<tr>
<td></td>
<td>iMC EAD 5.1 SP1 (E0301P03)</td>
</tr>
<tr>
<td></td>
<td>iMC QoS 5.1 SP1 (E0201)</td>
</tr>
<tr>
<td></td>
<td>iMC TAM 5.1 SP1 (E0301)</td>
</tr>
</tbody>
</table>
Sample: Display the version number of the software and boot ROM of the switch:

```
<4210>display version
3Com Corporation
3Com Switch 4210 PWR 9-Port Software Version 3.10 Release 2215P12  ------- Note①
Copyright (c) 2004-2012 3Com Corporation and its licensors, All rights reserved.
3Com Switch 4210 PWR 9-Port uptime is 0 week, 0 day, 0 hour, 4 minutes

3Com Switch 4210 PWR 9-Port with 1 Processor
64M bytes SDRAM
8M bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.A
Bootrom Version is 610  ------- Note②
CPLD Version is 003
[Subslot 0] 8FE+1Combo SFP Hardware Version is REV.A
```

**Restrictions and Cautions**

1) When enabling “unknown-multicast drop” function, the protocol packets whose destination IP addresses within 224.0.0.x~224.0.1.x will be dropped. If these protocol packets need to be processed, please do not enable this function.

2) Problems of packet forwarding and MIB statistics
   - The packets whose source MAC address is a multicast address or all-zero can be forwarded and the all-zero MAC address can be learned in ARL, but the zero MAC address cannot be displayed.
   - Wire-speed traffic from multiple ports is output through a half-duplex port and is not load shared, and error packets are counted. When traffic speed goes lower than the wire speed, above problems disappear.
   - Packets larger than 1518 bytes are counted as jumbo packets.
   - The etherStatsUndersizePkts MIB statistics are not precise for packets smaller than 64 bytes.

3) A version prior to R2215P12 might not support the cipher and simple keywords or use a different password encryption algorithm than R2215P12 or a later version. If you downgrade the software from R2215P12 or a later version to a version prior to R2215P12, or upgrade it to R2215P12 or a later version and roll it back after saving the configuration file, the relevant

### Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Web version</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>iNode version</td>
<td>iNode PC 5.1 (E0304)</td>
<td>The web file and application file (.bin) are two different files. Quidview and iMC should be purchased separately. When using Quidview to upgrade the device’s software, you need to select the latest software version manually.</td>
</tr>
<tr>
<td>Web version</td>
<td>s4p01_016</td>
<td></td>
</tr>
</tbody>
</table>
configuration commands might get lost or the passwords might become invalid. For more information, see the change descriptions for the commands.

Feature List

Hardware Features

Table 3 Hardware features (1)

<table>
<thead>
<tr>
<th>Item</th>
<th>Switch 4210 9-Port</th>
<th>Switch 4210 18-port</th>
<th>Switch 4210 26-port</th>
<th>Switch 4210 52-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H × W × D)</td>
<td>43.6mm × 230mm × 160mm (1.72 × 9.06 × 6.30 in.)</td>
<td>43.6mm × 360mm × 160mm (1.72 × 14.17 × 6.30 in.)</td>
<td>43.6mm × 440mm × 160mm (1.72 × 17.32 × 6.30 in.)</td>
<td>43.6mm × 440mm × 230mm (1.72 × 17.32 × 9.06 in.)</td>
</tr>
<tr>
<td>Physical dimensions (length × width × height)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>≤ 3 kg</td>
<td>≤ 3 kg</td>
<td>≤ 3 kg</td>
<td>≤ 5.5 kg</td>
</tr>
<tr>
<td>Service ports</td>
<td>8 10/100Base-TX ports and 1 Combo port</td>
<td>16 10/100Base-TX ports and 2 Combo ports</td>
<td>24 10/100Base-TX ports and 2 Combo ports</td>
<td>48 10/100Base-TX ports, 2 10/100/1000Base-TX ports and 2 SFP ports</td>
</tr>
<tr>
<td>Input voltage</td>
<td>AC:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rated voltage range: 100 VAC to 240 VAC (50Hz to 60Hz)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Voltage range: 90 VAC to 264 VAC (47Hz to 63Hz)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum power consumption</td>
<td>12W</td>
<td>15W</td>
<td>17W</td>
<td>24W</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>0°C to 45°C (32°F to 113°F)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating humidity</td>
<td>10% to 90%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4 Hardware features (2)

<table>
<thead>
<tr>
<th>Item</th>
<th>Switch 4210 PWR 9-port</th>
<th>Switch 4210 PWR 18-port</th>
<th>Switch 4210 PWR 26-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (H × W × D)</td>
<td>43.6mm × 300mm × 220mm (1.72 × 11.81 × 8.66 in.)</td>
<td>43.6mm × 300mm × 260mm (1.72 × 11.81 × 10.24 in.)</td>
<td>43.6mm × 440mm × 420mm (1.72 × 17.32 × 16.54 in.)</td>
</tr>
<tr>
<td>Physical dimensions (length × width × height)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>≤ 3 kg</td>
<td>≤ 3.5 kg</td>
<td>≤ 6.5 kg</td>
</tr>
<tr>
<td>Service ports</td>
<td>8 10/100Base-TX ports and 1 Combo port</td>
<td>16 10/100Base-TX ports and 2 Combo ports</td>
<td>24 10/100Base-TX ports and 2 Combo ports</td>
</tr>
</tbody>
</table>
Switch 4210 PWR 26-port supports both AC and DC(RPS) input, while the others just support AC input.

**AC:**
- Rated voltage range: 100 VAC to 240 VAC (50Hz to 60Hz)
- Max Voltage range: 90 VAC to 264 VAC (47Hz to 63Hz)

**DC(RPS):**
- Rated voltage range: -48V to -60V DC
- Max Voltage range: -36V to -72V DC

**Maximum power consumption**

<table>
<thead>
<tr>
<th></th>
<th>Switch 4210 PWR 9-port</th>
<th>Switch 4210 PWR 18-port</th>
<th>Switch 4210 PWR 26-port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>DC: 400W, PoE: 370W</td>
</tr>
</tbody>
</table>

**Operating temperature**

0°C to 45°C (32°F to 113°F)

**Operating humidity**

10% to 90%

## Software Features

**Table 5 Software features**

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching mode</td>
<td>Store and forward</td>
</tr>
<tr>
<td>VLAN</td>
<td>Up to 4K IEEE 802.1Q VLANs</td>
</tr>
<tr>
<td>VLAN interface</td>
<td>One VLAN interface</td>
</tr>
<tr>
<td>GVRP</td>
<td>Supported</td>
</tr>
<tr>
<td>Voice VLAN</td>
<td>Supported</td>
</tr>
<tr>
<td>Broadcast suppression</td>
<td>Broadcast suppression based on port bandwidth percentage</td>
</tr>
<tr>
<td></td>
<td>Storm constrain</td>
</tr>
<tr>
<td>Multicast</td>
<td>IGMP snooping</td>
</tr>
<tr>
<td></td>
<td>IGMP Snooping nonflooding</td>
</tr>
<tr>
<td>Unknown multicast drop</td>
<td>Supported</td>
</tr>
<tr>
<td>STP</td>
<td>STP/RSTP/MSTP</td>
</tr>
<tr>
<td>Link-aggregation</td>
<td>LACP</td>
</tr>
<tr>
<td></td>
<td>Manual aggregation</td>
</tr>
<tr>
<td></td>
<td>Up to 8 ports per aggregation group</td>
</tr>
<tr>
<td></td>
<td>Switch 4210 26-port and Switch 4210 PWR 26-port support up to 3 aggregation groups; the others support 2 aggregation groups.</td>
</tr>
<tr>
<td></td>
<td>Switch 4210 52-port supports up to 6 aggregation groups, each of which supports up to 8 ports.</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>Support one to multiple mirroring (one monitor port, multiple mirrored ports that are not limited)</td>
</tr>
<tr>
<td>Category</td>
<td>Features</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port isolate</td>
<td>Supported</td>
</tr>
<tr>
<td>Loopback-detection</td>
<td>Supported</td>
</tr>
<tr>
<td>Port internal and external loopback test</td>
<td>Supported</td>
</tr>
<tr>
<td>Port linkdown-delay</td>
<td>Supported</td>
</tr>
<tr>
<td>DLDP</td>
<td>Supported</td>
</tr>
<tr>
<td>LLDP</td>
<td>Supported</td>
</tr>
<tr>
<td>Smart Link</td>
<td>Supported</td>
</tr>
<tr>
<td>MAC address table</td>
<td>- Automatic MAC address learning</td>
</tr>
<tr>
<td></td>
<td>- Compliant with IEEE 802.1D</td>
</tr>
<tr>
<td></td>
<td>- Up to 8K MAC addresses</td>
</tr>
<tr>
<td></td>
<td>- Up to 1K static MAC addresses</td>
</tr>
<tr>
<td></td>
<td>- Dynamic and static unicast MAC addresses and black-hole MAC addresses supported</td>
</tr>
<tr>
<td>ARP</td>
<td>- ARP attack detection</td>
</tr>
<tr>
<td></td>
<td>- ARP packets rate limit</td>
</tr>
<tr>
<td>Flow-control</td>
<td>- IEEE 802.3x flow-control (full duplex)</td>
</tr>
<tr>
<td></td>
<td>- Back-pressure based flow control (half duplex)</td>
</tr>
<tr>
<td>Software upload and upgrade</td>
<td>Software upload and upgrade through the XMODEM protocol, FTP or TFTP</td>
</tr>
<tr>
<td>Management</td>
<td>CLI; Telnet; Console; SNMP; RMON 1,2,3,9 group MIB; HGMP V2; iMC network management; web network management; logging; alarming; IPv6 management</td>
</tr>
<tr>
<td>Quick startup</td>
<td>Supported</td>
</tr>
<tr>
<td>Maintenance</td>
<td>- Debugging</td>
</tr>
<tr>
<td></td>
<td>- ping, traceroute</td>
</tr>
<tr>
<td></td>
<td>- Telnet</td>
</tr>
<tr>
<td></td>
<td>- VCT</td>
</tr>
<tr>
<td></td>
<td>- Remote ping</td>
</tr>
<tr>
<td>Quick startup</td>
<td>Supported</td>
</tr>
<tr>
<td>QoS/ACL</td>
<td>- 4 output queues per port</td>
</tr>
<tr>
<td></td>
<td>- 802.1p priority, DSCP priority, IP precedence priority</td>
</tr>
<tr>
<td></td>
<td>- WRR and HQ+WRR queue scheduling</td>
</tr>
<tr>
<td></td>
<td>- Bidirectional rate limit per port with a granularity of 64 Kbps</td>
</tr>
<tr>
<td></td>
<td>- Flow traffic limit</td>
</tr>
<tr>
<td></td>
<td>- Traffic redirect</td>
</tr>
<tr>
<td></td>
<td>- Layer 2 ~Layer 7 packet filter, including: MAC address, MAC range, IP address, IP protocol, physical port, TCP/UDP port, VLAN, VLAN range etc.</td>
</tr>
<tr>
<td></td>
<td>- Different policy for matched ACL rule: permit/deny, traffic limit, traffic statistic, mirror, redirect, priority remark, queue scheduler</td>
</tr>
<tr>
<td></td>
<td>- Time range policy</td>
</tr>
<tr>
<td></td>
<td>- Qos-profile management for customization</td>
</tr>
</tbody>
</table>
### Category Features

**QinQ**
- User classification and password protection
- Guest VLAN
- IEEE 802.1X
- MAC based authentication
- Centralized MAC authentication
- AAA&Radius&HWTACACS authentication
- MAC Max learning number limit
- SSH 2.0
- Anti DoS attack
- MAC address black hole
- Password recovery
- BOOTROM access control
- IP+MAC+Port binding
- IP check
- Port Security
- RSA import key

**Security**
- DHCP Client
- DHCP Server
- DHCP Snooping
- DHCP option 82

**DHCP**
- NDP(Neighbor Discovery Protocol)
- NTDP(Network Topology Discovery Protocol)

**Cluster management**
- NDP(Neighbor Discovery Protocol)
- NTDP(Network Topology Discovery Protocol)

**NTP**
- Supported

**HGMP V2 stacking**
- Supported

---

### Version Updates

#### Feature Updates

**Table 6 Feature updates**

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMW310-R2215P12</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2215P11</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212P01</td>
<td>Hardware feature updates</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Software feature updates</td>
<td>1) Telnet fail trap</td>
</tr>
<tr>
<td>CMW310-R2212</td>
<td>Hardware feature updates</td>
<td>The first release, please refer to the manuals.</td>
</tr>
</tbody>
</table>
Command Line Updates

Table 7 Command line updates

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMW310-R2215P12</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>Command 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Syntax:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>local-user password-display-mode { auto</td>
</tr>
<tr>
<td></td>
<td></td>
<td>undo local-user password-display-mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>View : system view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Module of the command: AAA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The local-user password-display-mode command is not available to set the method for displaying local user passwords.</td>
</tr>
<tr>
<td>CMW310-R2215P11</td>
<td>New Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Deleted Commands</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Modified Commands</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212P01</td>
<td>New Commands</td>
<td>Please refer to the manuals.</td>
</tr>
</tbody>
</table>
## Deleted Commands

None

## Modified Commands

**Command 1**

**Syntax:**

```
mac-authentication timer offline-detect offline-detect-value
```

**View:** system view

Module of the command: MAC authentication

**Description:**

In before, the value range for the `offline-detect-value` argument is 1 to 65535 and now the value range for the `offline-detect-value` argument is 0 to 3000000. The offline detect timer configured in Ethernet port view takes precedence over the one configured in system view. If the `offline-detect-value` argument takes the value of 0, the offline detect timer is disabled.

## New Commands

CMW310-R2212

The first release, please refer to the manuals.

## Deleted Commands

None

## Modified Commands

None

## MIB Updates

### Table 8 MIB updates

<table>
<thead>
<tr>
<th>Version number</th>
<th>Item</th>
<th>MIB file</th>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMW310-R2215P12</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2215P12</td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2215P11</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2215P11</td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212P01</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212P01</td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212</td>
<td>New</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>CMW310-R2212</td>
<td>Modified</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Configuration Changes

Configuration Changes in CMW310-R2215P12

None

Configuration Changes in CMW310-R2215P11

Modified the value of node hh3cUserPassword in HH3C-USER-MIB due to security concerns. When read, hh3cUserPassword always returns a zero-length OCTET STRING.

Configuration Changes in CMW310-R2212P01

The changes in Operations of record WEB user

In early version:

The syslog records only the user's name after a WEB user log in, such as:

%Apr 7 09:10:24:698 2010 switch WEB/5/USER:- 1 -web login succeed

%Apr 7 09:10:47:961 2010 switch WEB/5/USER:- 1 -web logout

In current version:

The syslog records both the user's name and the user's IP address after a WEB user log in, such as:

%Apr 7 09:20:34:698 2010 switch WEB/5/USER:- 1 -web (1.1.1.1) login succeed

%Apr 7 09:20:37:961 2010 switch WEB/5/USER:- 1 -web (1.1.1.1) logout

The changes in Operations of ARP filter binding numbers on one port

In early version:

On one port, only one ARP filter binding item can be set to.

In current version:

On one port, eight ARP filter binding items can be set to.

The operation of ethernet type in loopback-detection packet

In early version:

The ethernet type in loopback-detection packet is 0x9000.

In current version:

The ethernet type in loopback-detection packet is 0x9001.

Configuration Changes in CMW310-R2212

None
Open Problems and Workarounds

None

List of Resolved Problems

Resolved Problems in CMW310-R2215P12

LSOD010584

- First Found-in Version: CMW310-R2215P11
- Condition:
  Configure password in ciphertext.
- Description:
  Because of the weak cryptographic algorithm there is a risk that the stored passwords possibly be cracked.

Resolved Problems in CMW310-R2215P11

LSOD010576

- First Found-in Version: CMW310-R2212P01
- Condition:
  Access the hh3cUserPassword node of hh3cUserInfoTable by SNMP.
- Description:
  When access the hh3cUserPassword node of hh3cUserInfoTable by SNMP, the device returns the user's password.

Resolved Problems in CMW310-R2212P01

LSOD10084

- First Found-in Version: CMW310-R2212
- Condition:
  Switch serves as DHCP snooping, and it receives bootp packets or abnormal DHCP packets without option 53.
- Description:
  Switch reboot abnormally.

LSOD10065

- First Found-in Version: CMW310-R2212
- Condition:
Configure 'pki certificate access-control-policy', then add and remove related certificate attribute access control rule.

- Description:
  Every operation will lead to 1056 bytes memory leak.

**LSOD09902**

- First Found-in Version: CMW310-R2212
- Condition:
  CPU is busy and there is a lot of trap information in a moment.
- Description:
  Device reboots abnormally.

**LSOD09931**

- First Found-in Version: CMW310-R2212
- Condition:
  Configured 'snmp-agent target-host trap address udp-domain A.B.C.D (D>223) params securityname RADAR' in system view.
- Description:
  Execute 'undo snmp-agent target-host A.B.C.D (D>223) securityname RADAR' unsuccessfully.

**ZDD03035**

- First Found-in Version: CMW310-R2212
- Condition:
  Some NMS send messages to the device at the same time.
- Description:
  The device can only process 10 messages in one time, others are dropped.

**LSOD10018**

- First Found-in Version: CMW310-R2212
- Condition:
  Switch serve as DHCP snooping, and it receives DHCP ACK packets with source UDP port 4011.
- Description:
  DHCP snooping can not transmit those DHCP ACK packets.

**LSOD10017**

- First Found-in Version: CMW310-R2212
- Condition:
  The device uses DC power.
- Description:
  There is 'Power 1: Get Temperature failed' while executing command 'display environment'.
LSOD09925

- First Found-in Version: CMW310-R2212
- Condition:

  Configure `authentication-mode scheme command-authorization` on VTY scheme. Telnet user passes RADIUS authentication and login the device.

- Description:

  After login, every command executed by user will cause memory leak.

LSOD09926

- First Found-in Version: CMW310-R2212
- Condition:

  The switch is enabled with DHCP snooping. The PXE client obtains an IP address through the switch, and downloads the bootstrap program and boot menu through the switch.

- Description:

  The PXE client can obtain an IP address successfully, but it fails to download the bootstrap program and boot menu.

LSOD09844

- First Found-in Version: CMW310-R2212
- Condition:

  In radius scheme, configure primary authentication server with IPv4 address, and secondary authentication server with IPv6 address. Do 802.1X authentication with RADIUS server. The 802.1X client uploads both IPv4 and IPv6 address simultaneously.

- Description:

  If primary server has no response, the device will do authentication with secondary server, but it can’t succeed.

LSOD09840

- First Found-in Version: CMW310-R2212
- Condition:

  Configure port-security userlogin-without mode and send Dot1x packet to the device.

- Description:

  The Dot1x packet causes the intrusion check which should not do like that.

LSOD09842

- First Found-in Version: CMW310-R2212
- Condition:

  Configure loopback-detection on the device and execute the “loopback interval” command.

- Description:

  Sometimes, the failure of “loopback interval” will occur.
**LSOD09873**

- First Found-in Version: CMW310-R2212
- Condition:

  Neither ‘dot1x authentication’ nor mac-authentication is enabled on the port. Only web-authentication is enabled. The user fails in authentication and enters the auth-fail VLAN.

- Description:

  The user ACL isn’t deleted after the user logs out from auth-fail VLAN.

**LSOD09865**

- First Found-in Version: CMW310-R2212
- Condition:

  Both the ‘mac-authentication’ and ‘mac-authentication guest-vlan’ are enabled on the port. User A is online, and user B tries to log in by ‘mac-authentication’.

- Description:

  User B can not pass the ‘mac-authentication’.

**LSOD09834**

- First Found-in Version: CMW310-R2212
- Condition:

  When an HGMP stack is established, two communities named public and private are automatically created for this stack. Create a new SNMP community named public or private, and associate an ACL with this community. Save the configuration. Then reboot the device, or disable and then enable the stack.

- Description:

  The SNMP community is not associated with an ACL.

**LSOD09895**

- First Found-in Version: CMW310-R2212
- Condition:

  In radius scheme, configure primary authentication server with an IPv4 address, and secondary authentication server with an IPv6 address. Do 802.1X authentication with RADIUS server, the 802.1X client upload both IPv4 and IPv6 address simultaneously.

- Description:

  If primary server has no response, the device will do authentication with secondary server, but it can’t succeed. The device reboots probably.

**LSOD09908**

- First Found-in Version: CMW310-R2212
- Condition:

  Connect S3100EI device with Quidway 5300 series device through fiber port. Reboot the S3100EI device or run for a long time.
- Description:
  Sometimes the fiber port can not linkup.

**LSOD09831**

- First Found-in Version: CMW310-R2212
- Condition:
  The client application does dot1x authentication with TTLS certification.
- Description:
  By chance, the device reboots abnormally for dead loop.

**LSOD09702**

- First Found-in Version: CMW310-R2212
- Condition:
  In radius scheme, configure primary authentication server with an IPv4 address, and secondary authentication server with an IPv6 address.
- Description:
  If primary server has no response, the device will do authentication with secondary server, but it can’t succeed.

**LSOD09755**

- First Found-in Version: CMW310-R2212
- Condition:
  The DLDP state of the port is active and the opposite port state is disabled.
- Description:
  The state-machine of DLDP switches between ‘disable’ and ‘active’, so the port goes up/down endless.

**LSOD09758**

- First Found-in Version: CMW310-R2212
- Condition:
  In the condition of IPv6 networks, a device works as SSH server, and the SSH client login and logout continuously.
- Description:
  Memory will leak. By the way, this problem is not found in the condition of IPv4 networks.

**LSOD09744**

- First Found-in Version: CMW310-R2212
- Condition:
  Port-security port-mode is userlogin-secure-or-mac or userlogin-secure-or-mac-ext, and the port-security guest-VLAN is the same as the MAC -authentication authorizing VLAN. A user enters the
port-security guest-VLAN because dot1x authentication fails or MAC-authentication fails, then passes the MAC-authentication and quits the port-security guest-VLAN.

- **Description:**
The user can not access the network.

**LSOD09733**

- **First Found-in Version:** CMW310-R2212
- **Condition:**
Configure an invalid user-defined IPv6 ACL rule, for example, a rule containing an incorrect subnet mask, at the web interface.

- **Description:**
The invalid rule is applied on the device successfully and included in the running configuration, but it does not take effect. The rule cannot survive a root, even if you have saved configuration.

**LSOD09807**

- **First Found-in Version:** CMW310-R2212
- **Condition:**
After the device rebooted, switch Combo port from copper to fiber.

- **Description:**
Occasionally, the fiber ports of some devices can not link up.

**LSOD09783**

- **First Found-in Version:** CMW310-R2212
- **Condition:**
Configure link-delay with X seconds on Combo port. Switch Combo port from copper to fiber and then switch from fiber to copper.

- **Description:**
There is no up down information of Combo port.

**LSOD09818**

- **First Found-in Version:** CMW310-R2212
- **Condition:**
After startup, the device tries to get configuration by DHCP auto configuration.

- **Description:**
During the device getting configuration, the network would be intermittent.

**LSOD09771**

- **First Found-in Version:** CMW310-R2212
- **Condition:**
Execute the command ‘loopback internal’ on port repeatedly.
• Description:
  Sometimes the loopback internal test would fail.

**LSOD09709**

• First Found-in Version: CMW310-R2212
• Condition:
  Configuring `authentication-mode scheme command-authorization` on the user interface, a user telneting the switch and login in successfully through local authentication mode, then the user running a valid command such as `quit` through telnet.
• Description:
  The device will be rebooted abnormally.

**LSOD09334**

• First Found-in Version: CMW310-R2212
• Condition:
  Disable DHCP function by system command 'undo dhcp enable'. Then set system clock.
• Description:
  The terminal will quit automatically.

**LSOD09596**

• First Found-in Version: CMW310-R2212
• Condition:
  Disable LLDP on device globally. Port X received LLDP packet.
• Description:
  The LLDP packet is forwarded to the other ports which should be discarded.

**Resolved Problems in CMW310-R2212**

None

**Related Documentation**

For the most up-to-date version of documentation:

1) Go to http://www.3Com.com/downloads
2) Select Documentation for Type of File and select Product Category.

**Software Upgrading**

⚠️ Caution

Upgrade software only when necessary and under the guidance of a technical support engineer.
The switch 4210 series, like switch 4210 9-Port (3CR17331-91), switch 4210 18-port (3CR17332-91), switch 4210 26-port (3CR17333-91), switch 4210 PWR 9-port (3CR17341-91), switch 4210 PWR 18-port (3CR17342-91) and switch 4210 PWR 26-port (3CR17343-91) can not use this version to upgrade the software.

If you want to upgrade the software on switch 4210 52-port (3CR17334-91) device, you must upgrade the bootrom to the current version first and then reboot the device. Upgrade the host software under the bootrom menu through FTP, TFTP or XModem.

Normally, the software of Switch 4210 is upgraded via serial port. However, this method is rather slow and very time-consuming. In addition, in this method, users either have to upgrade the switches at the installation sites or gather all the switches to upgrade one by one, whichever will consume enormous manpower. To solve the problem, 4210 Ethernet Switch uses the TFTP and FTP modules, which enable you to upgrade software and download files fast and flexibly.

**Remote Upgrading through CLI**

You may upgrade the application program and Boot ROM program of a device remotely through the command line interface (CLI). To this end, telnet to the device from a computer (at 10.10.110.1, for example) running FTP server first; and then get the application and Boot ROM program, switch.bin and switch.btm for example, from the FTP server as follows:

```
<H3C> ftp 10.10.110.1
Trying ...
Press CTRL+C to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):lyt
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get SWITCH.bin
[ftp] get SWITCH.btm
[ftp] bye
<H3C> boot bootrom SWITCH.btm
please wait ...
Bootrom is updated!
<H3C> boot boot-loader SWITCH.bin
<H3C> display boot-loader
The app to boot at the next time is: flash:/ SWITCH.bin
<H3C> reboot
```

After getting the new application file, reboot the device to validate it.

Note that if you do not have enough Flash space, upgrade the Boot ROM program first, and then download the application file to the device.

The following sections introduce some approaches to local upgrading.
Boot Menu

Upon power-on, the switch runs the Boot ROM program first. The following information will be displayed on the terminal:

Starting......

***********************************************************
*                                                           *
*       Switch 4210 PWR 9-Port BOOTROM, Version 610       *
*                                                           *
***********************************************************

Copyright(c) 2004-2010 3Com Corporation and its licensors.
Creation date   : Jul 21 2010, 17:00:56
CPU Clock Speed : 200MHz
BUS Clock Speed : 33MHz
Memory Size     : 64MB
Mac Address     : 000fe2004210

Press Ctrl-B to enter Boot Menu... 2

Note

After the screen displays “Press Ctrl-B to enter Boot Menu...”, you need to press <Ctrl+B> within 5 seconds to access the Boot menu. Otherwise, the system will start program decompression, and then you have to reboot the switch to access the Boot menu.

The system displays:

Password:

Enter the correct password (no password is set by default) to access the Boot menu.

Caution

Please keep in mind the modified Bootrom password.

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice (0-9):

Software Upgrading via Console Port (Xmodem Protocol)

Step1 Enter 1 in the Boot menu. Press <Enter> to access the download program menu.

Please set application file download protocol parameter:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return

Enter your choice (0-3): 3

Step2 Enter 3 to select the Xmodem protocol and press <Enter>. The following information appears:

Please select your download baudrate:
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. Return

Enter your choice (0-5):

Step3 Select the appropriate download baud rate. For example, enter 5 to select the download baud rate of 115200 bps. Press <Enter> and the following information appears:

Download baudrate is 115200 bps. Please change the terminal's baudrate to 115200 bps, and select XMODEM protocol.
Press ENTER key when ready.

Step4 Configure the same baud rate on the console terminal, disconnect the terminal and reconnect it. Then, press <Enter> to start downloading. The following information appears:

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

Downloading ... CCCCC
After the terminal baud rate is modified, it is necessary to disconnect and then re-connect the terminal emulation program to validate the new setting.

**Step 5** Select [Transfer\Send File] from the terminal window. Click <Browse> in the pop-up window and select the software to be downloaded. Select Xmodem from the Protocol drop down list.

![Figure 1 Send File](image)

**Step 6** Click <Send> and the following window appears.

![Figure 2 Xmodem File Send](image)

**Step 7** After downloading completes, the following information appears:

```
Loading ........................................................done
```
Software Upgrading via Ethernet Interface (FTP/TFTP)

Using TFTP Through an Ethernet Interface

1) Introduction to TFTP

The Trivial File Transfer Protocol (TFTP) employs UDP to provide unreliable data transfer service.

2) Upgrade procedure

Step1 Connect an Ethernet interface of the switch to the PC where the program files are located, and connect the console port of the switch to the same PC.

Step2 Run the TFTP server program on the PC, and put the program files into a file directory.

⚠️ Caution

4210 series switches are not shipped with the TFTP server program.

Step3 Run the terminal emulation program on the PC, and start the switch, to access the Boot menu.

Step4 Enter 1 in the Boot menu, and press <Enter> to enter the following menu.

Please set application file download protocol parameter:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return

Enter your choice(0-3):1

Step5 Enter 1 to use TFTP, and press <Enter>. The following information appears:

Please modify your TFTP protocol parameter:
Load File name
Switch IP address
Server IP address

Step6 Input correct information and press <Enter>. The following information appears:

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

Step7 Enter Y to start downloading the files. Enter N to return to the Boot menu. Take entering Y as an example. Enter Y and press <Enter>, the system begins downloading programs. After downloading completes, the system starts writing the programs to the flash. Upon completion of this operation, the screen displays the following information to indicate that the downloading is completed:

Loading ........................................................done
Writing to flash................................................done!
Using FTP Through an Ethernet Interface

1) Introduction to FTP

The 4210 can serve as an FTP server or client. In the following example, the 4210 serves as an FTP client.

2) Upgrade procedure

Step1 Connect an Ethernet interface of the 4800G to the PC where the program files are located, and connect the console port of the switch to the same PC.

Step2 Run the FTP server program on the PC, and put the program files into a file directory.

Step3 Run the terminal emulation program on the PC, and start the switch to access the Boot menu.

Step4 Enter 1 in the Boot menu and press <Enter> to access the following menu.

Please set application file download protocol parameter:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return

Enter your choice(0-3):2

Step5 Enter 2 to select FTP and press <Enter>. The following information appears:

Please modify your FTP protocol parameter:

Load File name
Switch IP address
Server IP address
FTP User Name
FTP User Password

Step6 Input correct information and press <Enter>. The following information appears:

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

Step7 Enter Y to start downloading the files. Enter N to return to the Boot menu. Take the first case as an example. Enter Y and press <Enter>, and the system begins downloading programs. After downloading completes, the system starts writing the programs into the flash. Upon completion of this operation, the screen displays the following information to indicate that the downloading is completed:

Loading ........................................................done
Writing to flash................................................done!

Please input the file attribute (main/backup/none): main

Appendix

Modified password setup and display for password/key-related security features.
For security purposes, all passwords and keys, including those configured in plaintext, are stored in encrypted form.

Details of Modified CLI Commands in R2215P12

bims-server

Old syntax

```plaintext
bims-server ip ip-address [ port port-number ] sharekey key
```

New syntax

```plaintext
bims-server ip ip-address [ port port-number ] sharekey [ cipher | simple ] key
```

Views

DHCP address pool view

Parameters

```plaintext
ip ip-address: Specifies the IP address of the BIMS server.
port port-number: Specifies the port number of the BIMS server, in the range of 1 to 65534.
cipher: Sets a ciphertext key.
simple: Sets a plaintext key.
key: Specifies the key string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 16 characters. If cipher is specified, it must be a ciphertext string of 1 to 53 characters. If neither cipher nor simple is specified, you set a plaintext key string.
```

Change description

Before modification: The cipher and simple keywords are not supported. The key you enter must be a plaintext string of 1 to 16 characters.

After modification: You can enter a key in encrypted form or plaintext form.

dhcp server bims-server

Old syntax

```plaintext
dhcp server bims-server ip ip-address [ port port-number ] sharekey key { interface interface-type interface-number | all } | to interface-type interface-number
```
New syntax

```
dhcp server bims-server ip ip-address [ port port-number ] sharekey [ cipher | simple ] key
{ interface interface-type interface-number [ to interface-type interface-number ] | all }
```

Views

System view

Parameters

- **ip ip-address**: Specifies the IP address of the BIMS server.
- **port port-number**: Specifies the port number of the BIMS server, in the range of 1 to 65534.
- **cipher**: Sets a ciphertext key.
- **simple**: Sets a plaintext key.
- **key**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.
- **interface interface-type interface-number [ to interface-type interface-number ]**: Specifies an interface range. The **interface-type interface-number** arguments specify an interface by its type and number.
- **all**: Specifies all interfaces.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key you enter must be a plaintext string of 1 to 16 characters.

After modification: You can enter a key in encrypted form or plaintext form.

**dldp authentication-mode**

Old syntax

```
dlldp authentication-mode { none | simple simple-password | md5 md5-password }
```

New syntax

```
dlldp authentication-mode { none | { simple | md5 } password }
```

Views

System view
Parameters

**none**: Specifies not to perform authentication.

**simple**: Specifies the simple authentication mode and sets a plaintext or ciphertext password.

**md5**: Specifies the MD5 authentication mode and sets a plaintext or ciphertext password.

**password**: Sets the password. This argument is case sensitive. It must be a plaintext string of 1 to 16 characters, or a ciphertext string of 33 to 53 characters.

Change description

Before modification:
- For simple authentication, you can set only a plaintext password of 1 to 16 characters.
- For MD5 authentication, you can set a plaintext or ciphertext password. A plaintext password comprises 1 to 16 characters, and a ciphertext password is a ciphertext string corresponding to the plaintext password.

After modification: Both simple authentication and MD5 authentication support plaintext or ciphertext passwords. A plaintext password is a string of 1 to 16 characters, and a ciphertext password is a string of 33 to 53 characters.

**key (HWTACACS scheme view)**

Old syntax

```
key { accounting | authentication | authorization } string
```

New syntax

```
key { accounting | authentication | authorization } [ cipher | simple ] string
```

View

HWTACACS scheme view

Parameters

**accounting**: Sets the key for secure HWTACACS accounting communication.

**authentication**: Sets the key for secure HWTACACS authentication communication.

**authorization**: Sets the key for secure HWTACACS authorization communication.

**cipher**: Sets a ciphertext key.

**simple**: Sets a plaintext key.

**string**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.
Change description

Before modification: The cipher and simple keywords are not supported. The key for securing HWTACACS authentication, authorization, or accounting communication must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure HWTACACS authentication, authorization, or accounting communication.

key (RADIUS scheme view)

Old syntax

key { accounting | authentication } string

New syntax

key { accounting | authentication } { cipher | simple } string

View

RADIUS scheme view

Parameters

accounting: Sets the key for secure RADIUS accounting communication.

authentication: Sets the key for secure RADIUS authentication/authorization communication.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

string: Specifies the key string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 16 characters. If cipher is specified, it must be a ciphertext string of 1 to 53 characters. If neither cipher nor simple is specified, you set a plaintext key string.

Change description

Before modification: The cipher and simple keywords are not supported. The key for securing RADIUS authentication/authorization or accounting communication must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure RADIUS authentication/authorization or accounting communication.

local-server nas-ip

Old syntax

local-server nas-ip ip-address key password
New syntax

```
local-server nas-ip ip-address key [ cipher | simple ] password
```

View

System view

Parameters

- **nas-ip ip-address**: Specifies the IP address of the network access server through which users can access the local RADIUS authentication/authorization server. The IP address must be in dotted decimal notation.

- **key [ cipher | simple ] password**: Sets the key to share between the local RADIUS authentication/authorization server and the network access server.
  - **cipher**: Sets a ciphertext key.
  - **simple**: Sets a plaintext key.
  - **password**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Change description

Before modification: The **cipher** and **simple** keywords are not supported. The key to share between the local RADIUS authentication/authorization server and the network access server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to share between the local RADIUS authentication/authorization server and the network access server.

```
mac-authentication authmode usernameasMACaddress
```

Old syntax

```
mac-authentication authmode usernameasMACaddress [ usernameformat { with-hyphen | without-hyphen } { lowercase | uppercase } | fixedpassword password ]
```

New syntax

```
mac-authentication authmode usernameasMACaddress [ usernameformat { with-hyphen | without-hyphen } { lowercase | uppercase } | fixedpassword [ cipher | simple ] password ]
```

View

System view

Parameters

- **usernameformat**: Specifies the username and password input format for MAC-based accounts.
**with-hyphen**: Uses the hyphenated MAC address of a user, such as 00-05-e0-1c-02-e3, as the username and password for MAC authentication of the user.

**without-hyphen**: Uses the unhyphenated MAC address of a user, such as 0005e01c02e3, as the username and password for MAC authentication of the user.

**lowercase**: Enters letters of the MAC address in lower case.

**uppercase**: Enters letters of the MAC address in upper case.

**fixedpassword** [ simple | cipher ] **password**: Uses a fixed password, instead of user MAC addresses, for MAC authentication users.

- **cipher**: Sets a ciphertext password.
- **simple**: Sets a plaintext password.
- **password**: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password.

**Change description**

Before modification: The **cipher** and **simple** keywords are not supported. The password you enter must be a plaintext string.

After modification: You can enter a password in encrypted form or plaintext form.

**mac-authentication authpassword**

**Old syntax**

```
mac-authentication authpassword password
```

**New syntax**

```
mac-authentication authpassword [ cipher | simple ] password
```

**View**

System view

**Parameters**

- **[ cipher | simple ] password**: Sets the password of the shared account for MAC authentication users.
  - **cipher**: Sets a ciphertext password.
  - **simple**: Sets a plaintext password.
  - **password**: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password.
Change description

Before modification: The cipher and simple keywords are not supported. The password you enter must be a plaintext string.

After modification: You can enter a password in encrypted form or plaintext form.

ntp-service authentication-keyid

Old syntax

ntp-service authentication-keyid keyid authentication-mode md5 value

New syntax

ntp-service authentication-keyid keyid authentication-mode md5 [ cipher | simple ] value

View

System view

Parameters

keyid: Specifies a key ID in the range of 10 to 4294967295.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

value: Specifies the key string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 32 characters. If cipher is specified, it must be a ciphertext string of 1 to 73 characters. If neither cipher nor simple is specified, you set a plaintext key string.

Change description

Before modification: The cipher and simple keywords are not supported. The key you enter must be a plaintext string of 1 to 32 characters.

After modification: You can enter a key in encrypted form or plaintext form.

password (Remote-ping test group view)

Old syntax

password password

New syntax

password [ cipher | simple ] password
View

Remote-ping test group view

Parameters

cipher: Sets a ciphertext FTP password.
simple: Sets a plaintext FTP password.

password: Specifies the password string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 32 characters. If cipher is specified, it must be a ciphertext string of 1 to 73 characters. If neither cipher nor simple is specified, you set a plaintext password string.

Change description

Before modification: The cipher and simple keywords are not supported. The FTP password must be a plaintext string of 1 to 32 characters.

After modification: You can set an FTP password in encrypted form or plaintext form.

password (local user view)

Syntax

password [{ cipher | simple } password ]

View

Local user view

Parameters

cipher: Sets a ciphertext password.
simple: Sets a plaintext password.

password: Specifies the password string. This argument is case sensitive.

- If simple is specified, it is a plaintext string of 1 to 63 characters.
- If cipher is specified, it is a string of 1 to 117 characters. If you specify a password of 1 to 63 characters and the system can decrypt the password, the system considers that you have specified a ciphertext password. If you specify a password of 1 to 63 characters but the system cannot decrypt the password, the system considers that you have specified a plaintext password. A password comprising 64 to 117 characters is always considered a ciphertext password.

Change description

Before modification: If cipher is specified, you can set an 88-character password or a password of 1 to 63 characters.

After modification: If cipher is specified, you can set a password of 1 to 117 characters.
primary accounting (RADIUS scheme view)

Old syntax

```
primary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
```

New syntax

```
primary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]
```

View

RADIUS scheme view

Parameters

- `ip-address`: Specifies the IPv4 address of the primary RADIUS accounting server.
- `ipv6 ipv6-address`: Specifies the IPv6 address of the primary RADIUS accounting server.
- `port-number`: Specifies the service port number of the primary RADIUS accounting server, a UDP port number in the range of 1 to 65535.

`key [ cipher | simple ] string`: Sets the key for secure communication with the primary RADIUS accounting server.

- `cipher`: Sets a ciphertext key.
- `simple`: Sets a plaintext key.
- `string`: Specifies the key string. This argument is case sensitive. If `simple` is specified, it must be a string of 1 to 16 characters. If `cipher` is specified, it must be a ciphertext string of 1 to 53 characters. If neither `cipher` nor `simple` is specified, you set a plaintext key string.

Change description

Before modification: The `cipher` and `simple` keywords are not supported. The key for securing communication with the primary RADIUS accounting server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the primary RADIUS accounting server.

primary authentication (RADIUS scheme view)

Old syntax

```
primary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]
```

New syntax

```
primary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]
```
View

RADIUS scheme view

Parameters

`ip-address`: Specifies the IPv4 address of the primary RADIUS authentication/authorization server.

`ipv6 ipv6-address`: Specifies the IPv6 address of the primary RADIUS authentication/authorization server.

`port-number`: Specifies the service port number of the primary RADIUS authentication/authorization server, a UDP port number in the range of 1 to 65535.

`key [ cipher | simple ] string`: Sets the key for secure communication with the primary RADIUS authentication/authorization server.

- `cipher`: Sets a ciphertext key.
- `simple`: Sets a plaintext key.
- `string`: Specifies the key string. This argument is case sensitive. If `simple` is specified, it must be a string of 1 to 16 characters. If `cipher` is specified, it must be a ciphertext string of 1 to 53 characters. If neither `cipher` nor `simple` is specified, you set a plaintext key string.

Change description

Before modification: The `cipher` and `simple` keywords are not supported. The key for securing communication with the primary RADIUS authentication/authorization server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the primary RADIUS authentication/authorization server.

secondary accounting (RADIUS scheme view)

Old syntax

`secondary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]`

New syntax

`secondary accounting { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]`

View

RADIUS scheme view

Parameters

`ip-address`: Specifies the IPv4 address of the secondary RADIUS accounting server.

`ipv6 ipv6-address`: Specifies the IPv6 address of the secondary RADIUS accounting server.
port-number: Specifies the service port number of the secondary RADIUS accounting server, a UDP port number in the range of 1 to 65535.

key [ cipher | simple ] string: Sets the key for secure communication with the primary RADIUS accounting server.

- cipher: Sets a ciphertext key.
- simple: Sets a plaintext key.
- string: Specifies the key string. This argument is case sensitive. If simple is specified, it must be a string of 1 to 16 characters. If cipher is specified, it must be a ciphertext string of 1 to 53 characters. If neither cipher nor simple is specified, you set a plaintext key string.

Change description

Before modification: The cipher and simple keywords are not supported. The key for securing communication with the secondary RADIUS accounting server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the secondary RADIUS accounting server.

secondary authentication (RADIUS scheme view)

Old syntax

secondary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key string ]

New syntax

secondary authentication { ip-address | ipv6 ipv6-address } [ port-number ] [ key [ cipher | simple ] string ]

View

RADIUS scheme view

Parameters

ip-address: Specifies the IPv4 address of the secondary RADIUS authentication/authorization server.

ipv6 ipv6-address: Specifies the IPv6 address of the secondary RADIUS authentication/authorization server.

port-number: Specifies the service port number of the secondary RADIUS authentication/authorization server, a UDP port number in the range of 1 to 65535.

key [ cipher | simple ] string: Sets the key for secure communication with the secondary RADIUS authentication/authorization server.

- cipher: Sets a ciphertext key.
- simple: Sets a plaintext key.
• **string**: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

**Change description**

Before modification: The **cipher** and **simple** keywords are not supported. The key for securing communication with the secondary RADIUS authentication/authorization server must be a plaintext string of 1 to 16 characters.

After modification: You can set a key in encrypted form or plaintext form to secure communication with the secondary RADIUS authentication/authorization server.

**set authentication password**

**Syntax**

```
set authentication password { simple | cipher } password
```

**View**

User interface view

**Parameters**

**cipher**: Sets a ciphertext password.

**simple**: Sets a plaintext password.

**key**: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a plaintext string of 1 to 16 characters. If **cipher** is specified, it can be a plaintext string of 1 to 16 characters or a ciphertext string of 17 to 53 characters.

**Change description**

Before modification: When you specify the **cipher** keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password.

After modification: When you specify the **cipher** keyword, you can enter a string of 1 to 53 characters as the password.

**snmp-agent usm-user v3**

**Syntax**

```
snmp-agent usm-user v3 user-name group-name [ [ cipher ] authentication-mode { md5 | sha } auth-password [ privacy-mode { aes128 | des56 } priv-password ] ] [ acl acl-number ]
```

**View**

System view
Parameters

user-name: Specifies a username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies a group name, a case-sensitive string of 1 to 32 characters.

cipher: Specifies that auth-password and priv-password are encrypted keys, which can be calculated to a hexadecimal string by using the snmp-agent calculate-password command. If this keyword is not specified, auth-password and priv-password are plaintext keys.

authentication-mode: Specifies an authentication algorithm. MD5 is faster but less secure than SHA. For more information about these algorithms, see Security Configuration Guide.

- md5: Specifies the MD5 authentication algorithm.
- sha: Specifies the SHA-1 authentication algorithm.

auth-password: Specifies a case-sensitive plaintext or encrypted authentication key. A plaintext key is a string of 1 to 64 visible characters. If the cipher keyword is specified, the encrypted authentication key length requirements differ by authentication algorithm and key string format, as shown in Table 9.

<table>
<thead>
<tr>
<th>Authentication algorithm</th>
<th>Hexadecimal string</th>
<th>Non-hexadecimal string</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>32 characters</td>
<td>53 characters</td>
</tr>
<tr>
<td>SHA</td>
<td>40 characters</td>
<td>57 characters</td>
</tr>
</tbody>
</table>

privacy-mode: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- des56: Specifies the DES algorithm.
- aes128: Specifies the AES algorithm.

priv-password: Specifies a case-sensitive plaintext or encrypted privacy key. A plaintext key is a string of 1 to 64 characters. If the cipher keyword is specified, the encrypted privacy key length requirements differ by authentication algorithm and key string format, as shown in Table 10.

<table>
<thead>
<tr>
<th>Authentication algorithm</th>
<th>Encryption algorithm</th>
<th>Hexadecimal string</th>
<th>Non-hexadecimal string</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>AES128 or DES-56</td>
<td>32 characters</td>
<td>53 characters</td>
</tr>
<tr>
<td>SHA</td>
<td>AES128 or DES-56</td>
<td>40 characters</td>
<td>53 characters</td>
</tr>
</tbody>
</table>

acl acl-number: Specifies a basic ACL to filter NMSs by source IPv4 address. The acl-number argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

local: Represents a local SNMP entity user.

engineid engineid-string: Specifies an SNMP engine ID as a hexadecimal string. The engineid-string argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.
Change description

Before modification: Only authentication and privacy keys in hexadecimal format are supported.

After modification: Both hexadecimal and non-hexadecimal format authentication and privacy keys are supported.

- For encrypted authentication key length requirements, see Table 9.
- For encrypted privacy key length requirements, see Table 10.

super password

Syntax

super password [ level user-level ] { cipher | simple } password

Views

System view

Parameters

level user-level: Specifies a user privilege level in the range of 1 to 3. The default is 3.

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

key: Specifies the password string. This argument is case sensitive. If simple is specified, it must be a plaintext string of 1 to 16 characters. If cipher is specified, it can be a plaintext string of 1 to 16 characters or a ciphertext string of 17 to 53 characters.

Change description

Before modification: When you specify the cipher keyword, you can enter a string of 1 to 16 characters or a string of 24 characters as the password.

After modification: When you specify the cipher keyword, you can enter a string of 1 to 53 characters as the password.