H3C S3610_5510-CMW520-R5319P08

Release Notes

H3C

ITolP Solutions Expert

H3C S3610_5510-CMW520-R5319P08 Release Notes

Keywords: Version, feature, change, defect, upgrading.

Abstract: Version Information, Unresolved Problems and Avoidance Measures, software upgrading.

Abbreviations:

Abbreviations	Full spelling
CMW	Comware
MIB	Management Information Base
ACL	Access Control List
NMF	Network Management Framework
NCC	Network Configuration Center
GARP	General Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
RRPP	Rapid Ring Protection Protocol
OAM	Operation, Administration and Maintenance
DLDP	Device Link Detection Protocol
EAD	Endpoint Admission Defense

Table of Contents

List of Tables

Version Information

Version Number

Version Information: Comware Software, Version 5.20, Release 5319P08

Note: This version number can be displayed by command **display version** under any view. Please see **Note 1**

Version History

Table 1 Version history

Version Number	Based Version Number	Release Date	Remark
S3610_5510-CMW520-R5319P08	S3610_5510-CMW520-R5319P06	2014-07-03	Modify bugs
S3610_5510-CMW520-R5319P06	S3610_5510-CMW520-R5319P05	2013-10-08	Modify bugs
S3610_5510-CMW520-R5319P05	S3610_5510-CMW520-R5319P04	2013-06-24	Modify bugs
S3610_5510-CMW520-R5319P04	S3610_5510-CMW520-F5319P03	2013-01-10	Support new features
S3610_5510-CMW520-F5319P03	S3610_5510-CMW520-F5319P02	2013-01-08	Modify bugs
S3610_5510-CMW520-F5319P02	S3610_5510-CMW520-F5318P02	2012-11-29	Modify bugs
S3610_5510-CMW520-F5318P02	S3610_5510-CMW520-F5318P01	2012-10-19	Modify bugs
S3610_5510-CMW520-F5318P01	S3610_5510-CMW520-F5317	2011-11-16	Modify bugs
S3610_5510-CMW520-F5317	S3610_5510-CMW520-F5316	2011-01-25	Support new features
S3610_5510-CMW520-F5316	S3610_5510-CMW520-F5315	2010-07-29	Support new features
S3610_5510-CMW520-F5315	S3610_5510-CMW520-F5310	2010-03-23	Support new features
S3610_5510-CMW520-F5310	S3610_5510-CMW520-R5309P02	2009-09-18	Support new features
S3610_5510-CMW520-R5309P02	S3610_5510-CMW520-R5309	2009-06-17	Modify bugs
S3610_5510-CMW520-R5309	S3610_5510-CMW520-R5308	2009-04-03	Modify bugs

Version Number	Based Version Number	Release Date	Remark
S3610_5510-CMW520-R5308	S3610_5510-CMW520-R5306	2009-03-26	Modify bugs
S3610_5510-CMW520-R5306	S3610_5510-CMW520-F5305P06	2009-01-12	Support new feature
S3610_5510-CMW520-F5305P06	S3610_5510-CMW520-F5305P02	2008-11-21	Support new feature
S3610_5510-CMW520-F5305P02	S3610_5510-CMW520-R5303P01	2008-07-02	Support new feature
S3610_5510-CMW520-R5303P01	S3610_5510-CMW520-R5303	2008-03-30	Optimization Packets receiving and sending
S3610_5510-CMW520-R5303	S3610_5510-CMW520-F5302P01	2008-3-12	Support new hardware
S3610_5510-CMW520-F5302P01	S3610_5510-CMW520-F5302	2007-12-18	Modify bug.
S3610_5510-CMW520-F5302	S3610_5510-CMW520-R5301	2007-10-30	Modify bug. Add new features.
S3610_5510-CMW520-R5301	S3610_5510-CMW520-R0001P02	2007-8-27	None
S3610_5510-CMW520-R0001P02	S3610_S5510-CMW520-R0001	2007-5-28	None
S3610_S5510-CMW520-R0001	S3610_S5510-CMW520-E0001	2006-11-21	None
S3610_S5510-CMW520-E0001	First time.	2006-7-28	None

Hardware and Software Compatibility Matrix

Table 2 Hardware and software compatibility matrix

Hardware Platform	S3610&S5510 series
Equipment Model	S3610-52P/S3610-28TP/S3610-28F/S3610-28P/S5510-24F/S5510-24P/S3610-52M
Memory Requirement	Min 128M
Flash Requirement	Min 32M

Boot ROM Version	Version 210 or later (Note: This version number can be displayed by command display version under any view. Please see Note2)
Host Software	S3610_5510-CMW520-R5319P08.bin
iMC Version	iMC PLAT 7.0 (E0202P03) iMC EAD 7.0(E0202) iMC NTA 7.0 (E0201P02) iMC QoSM 7.0 (E0201H01) iMC SHM 7.0 (E0202L01) iMC EIA7.0 (E0203)
iNode	iNode PC 7.0 (E0203)

```
<H3C>display version
H3C Comware Platform Software
Comware Software, Version 5.20, Release 5319P08   ------- Note 1
Copyright (c) 2004-2014 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C S3610-52P uptime is 0 week, 0 day, 0 hour, 2 minutes

H3C S3610-52P
128M     bytes DRAM
16M      bytes Flash Memory
Config Register points to FLASH

Hardware Version is REV.A
CPLD Version is CPLD 001
Bootrom Version is 213                        -------- Note 2
[SubSlot  0] 48FE Hardware Version is REV.A
[SubSlot  1]  4GE Hardware Version is REV.A
```

Restrictions and Cautions

- The FE ports will up and down frequently, if they are connected with different speed in forced mode;
- The redirected packets are always untagged;
- The last fragmented IP packet cannot be controlled by ACL;
- The ports, on which 802.1X is enabled, just control the inbound packets.
- The newly bought switch with the embedded application in version R5303 is prohibited to down-grade to lower version due to the compatibility between the new hardware and the software.
- For S3610-52M, the Sub Cards MUST NOT be plugged in or pulled out when power is on.
- The application of F5305P02 and its later version cannot work with Bootrom earlier than version 142(not include 142). So, if upgrade to F5305P02 and later version. The Bootrom must be upgraded first or together with application software according to Version Compatibility Table.

Feature List

Hardware Features

Table 3 Hardware features

Item	H3C S3610 series
Dimensions (H × W × D)	S3610: 43.6 × 440 × 260 mm (1.7 × 17.3 × 10.2 in) S5510: 43.6 × 440 × 360 mm (1.7 × 17.3 × 14.2 in) S3610-52M: 86×436×390mm(3.35 × 17.14 × 15.3 in)
Weight	S3610-52P: 3.8KG S3610-28P: 3.6KG S3610-28TP: 3.7KG S3610-28F: 3.8KG S3610-52M: 8.5KG S5510 without power modules: 4.6 kg S5510 power module: 0.8 kg to 1 kg per
Management port	One Console port
Service port	S3610-28P: 24 × 10/100 Mbps electrical ports + 4 × 1,000 Mbps SFP ports S3610-28TP: 24 × 10/100 Mbps electrical ports + 2 × 1,000 Mbps SFP ports + 2 × 10/100/1,000 Mbps electrical ports S3610-52P: 48 × 10/100 Mbps electrical ports + 4 × 1,000 Mbps SFP ports S3610-28F: 24 × 100 Mbps SFP ports + 2 × 1,000 Mbps SFP ports + 2 × 10/100/1,000 Mbps electrical ports S5510-24P-AC/S5510-24P-DC: 24 × 10/100/1000 Mbps electrical ports + 4 Gigabit SFP ports (Combo) S5510-24F-AC/S5510-24F-DC: 24 Gigabit SFP ports + 4 × 10/100/1,000 Mbps electrical ports(Combo) S3610-52M: Decided by the inserted modules. Up to 48 × 10/100 Mbps electrical ports or 48 × 100 Mbps SFP ports. On the rear panel, there are 4 × 1000 Mbps fixed SFP ports and 4 × 10/100/1000 Mbps fixed electrical ports.
Input voltage	AC: Rated voltage range: 100 VAC to 240 VAC; 50 Hz or 60 Hz Max voltage range: 90 VAC to 264 VAC; 50 Hz or 60 Hz DC: Rated voltage range: -48 V to -60 V Max voltage range: -36 V to -72 V

Item	H3C S3610 series
Power consumption (full load)	S3610-52P: 45 W S3610-28P: 35 W S3610-28TP: 40 W S3610-28F: 60 W S3610-52M: 110W S5510-24P-AC/S5510-24P-DC: 80W S5510-24F-AC/S5510-24F-DC: 75W
Operating temperature	0°C to 45°C (32°F to 113°F)
Relative humidity (no condensing)	10% to 90%

Software Features

Table 4 Software features

Feature	Power supply
Wire speed L2/L3 forwarding	S3610: Switching capacity (28 ports/52 ports): 12.8 Gbps/17.6 Gbps S3610: Packet forwarding rate (28 ports/52 ports):9.53 Mpps/13.1 Mpps S5510: Switching capacity: 48 Gbps S5510: Packet forwarding rate: 35.71 Mpps
Link Aggregation	Supports aggregation of Fast Ethernet (FE) ports Supports aggregation of Gigabit Ethernet (GE) ports Supports static link aggregation Supports dynamic link aggregation
MAC address	Supports 16 K MAC addresses Supports MAC address black hole Supports MAC address learning limit
Port	Supports IEEE 802.3x flow control (full-duplex) Supports Back-pressure based flow control (half duplex) Supports port-based broadcast suppression Supports port priority settings Supports Storm Constrain Supports port bridge function
PPPoE Agent	Suports PPPoE Agent
OAM	Supports OAM 802.3ah

Feature	Power supply
VLAN	Supports port-based VLANs (4,094 VLANs) Supports protocol-based VLANs Supports VLANs based on IPv4 subnets Supports Voice VLANs Supports GVRP/GARP Supports VLAN VPN(QinQ), Selective QinQ and BPDU tunnel Supports VLAN Translation Supports VLAN Mapping Supports SuperVLAN Supports isolate-user-VLAN
DHCP	Supports DHCP Server(MCE supported) Supports DHCP-Relay(MCE supported) Supports DHCP Client Supports DHCP Snooping Supports DHCP Snooping for Option82 Supports DHCPv6 Snooping
UDP Helper	Supports UDP Helper
DNS	Supports static domain name resolution Supports dynamic DNS client
ARP	Supports ARP Supports gratuitous ARP Supports ARP Proxy Supports ARP Detection Supports ARP Snooping Supports MFF (MAC-Forced Forwarding)
IP routing	Supports static route and default route Supports Routing Information Protocol (RIP) v1/v2 Supports RIPng Supports Open Shortest Path First (OSPF) v1/v2 Supports OSPFv3 Supports IS-IS Supports IS-ISv6 Supports Border Gateway Protocol (BGP) Supports for BGP4+ for IPV6 Supports equivalent route Supports routing policy Supports BFD for static route

Feature	Power supply	
Multicast	Supports Internet Group Management Protocol (IGMP) Snooping	
	Supports IGMPv1/v2/v3	
	Supports Protocol Independent Multicast-Dense Mode (PIM-DM)	
	Supports Protocol Independent Multicast-Sparse Mode (PIM-SM)	
	Supports Multicast Source Discovery Protocol (MSDP)	
	Supports MLD Snooping	
	Supports MLDv2 Snooping	
	Supports dropping unknown IPv4 multicast data	
	Supports dropping unknown IPv6 multicast data	
	Supports IPv6 PIM-DM	
	Supports IPv6 PIM-SSM	
	Supports IPv6 PIM-SM	
	Supports IPv6 Multicast VLAN+	
	Supports IGMP Snooping Group Policy	
	Supports MLD Snooping Group Policy	
Layer2 loop free protocols	Supports STP/RSTP/MSTP	
	Supports RRPP	
	Supports Smart Link	
IPV6	Supports Neighbor Discovery (ND)	
	Supports PMTU	
	Supports IPv6 Ping and IPv6 Tracert	
	Supports IPv6 Telnet	
	Supports IPv6 TFTP	
	Supports IPv6 ND Snooping	
	Supports IPv6 ND Detection	
IPv6 over IPv4 Tunnel	Supports manual Tunnel configuration	
	Supports 6to4 tunnel	
	Supports ISATAP(Intra-site Automatic Tunneling Protocol) tunnel	
	Supports Auto-tunnel (namely, IPv4 compatible tunnel)	
QoS/ACL	Supports ACLs	Supports traffic classification based on source MAC address, destination MAC address, source IP address, destination IP address, Layer 4 port, protocol type, VLAN, and so on
		Supports basic ACL
		Supports advanced ACL
		Supports L2 ACL
		Supports user-defined ACL
	Supports ACL flow template	Supports user-defined flow template
		Supports default flow template

Feature	Power supply	
	Supports QoS	Flow-based traffic rate limit
		Supports flow-based priority tag
		Flow-based packet VLAN ID change
		Flow-based redirection of packets to another port or IP next hop
		Flow-based traffic statistics
		Flow-based traffic mirroring
		Supports SP/WRR/SP+WRR queue scheduling
		Supports port mirroring and RSPAN (remote port mirroring)
		Supports port traffic shaping
		Supports congestion avoidance and drop policies
	Supports IPv6 ACLs	Supports traffic classification based on source IPv6 address, destination IPv6 address, Layer 4 port, protocol type, and so on
		Supports basic IPv6 ACL
		Supports advanced IPv6 ACL
	Supports Time Range	
	Supports Routing Policy	
	Supports IP Source Guard	
	Supports IPv6 Source Guard	
	Supports applying a QoS policy to a user profile	
Security Features	Supports hierarchical management and password protection of users	
	Supports IEEE 802.1X authentication	
	Supports AAA	
	Supports RADIUS authentication	
	Supports HWTacacs	
	Supports centralized MAC address based authentication	
	Supports port isolation	
	Supports IP + MAC + port binding	
	Supports HTTPS	
	Supports EAD	
	Supports Port Security	
	Supports System-Guard	
	Supports Password Control	
Reliability	Supports Virtual Redundancy Routing Protocol (VRRP)	
	Supports Bidirectional Forwarding Detection (BFD)	
	Supports Connectivity Fault Detection (CFD)	
	Supports Track	
	Supports Graceful Restart(GR)	
Loading and upgrade	Supports loading and upgrade through XModem protocol	
	Supports loading and upgrade through file transfer protocol (FTP)	
	Supports loading and upgrade through trivial file transfer protocol (TFTP)	

Feature	Power supply
Management	Supports configuration through the Command line interface (CLI) Supports configuration through Telnet Supports configuration through Console port Supports Simple Network Management Protocol (SNMP) v1/v2c/v3 Supports Remote Monitoring (RMON) 1/2/3/9 groups of MIBs Supports QuidView NMS Supports Web-based network management Supports system log Supports hierarchical alarms Supports HGMP v2 Supports remote dialing through modem Supports NTP Supports SSH Supports SSHv2.0 Supports power supply status detection and alarms Supports sFlow Supports LLDP
Maintenance	Supports Debugging Information Output Supports PING and Tracert Supports NQA Supports remote maintenance through Telnet Supports Virtual Cable Test

Version Updates

Feature Updates

Table 5 Feature updates

Version Number	Item	Description
S3610_5510-CMW520-R5319P08	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-R5319P06	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None

Version Number	Item	Description
S3610_5510-CMW520-R5319P05	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-R5319P04	Changed Hardware Features	New Features: 1. CC/FIPS 2. Disabling password recovery capacity Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-F5319P03	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-F5319P02	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-F5318P02	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-F5318P01	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. DHCP option82 sub 1/2/9 Deleted Features: None
S3610_5510-CMW520-F5317	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 2. Isolate-user-VLAN configuration restrictions removed 3. PPPoE Agent 4. IRF LITE supports non-SFP-STACK-Kit module. 5. Support IPv4 ACL rule remark.
S3610_5510-CMW520-F5316	Changed Hardware Features	New Features: None Deleted Features: None

Version Number	Item	Description
	Changed Software Features	New Features: 1. isolate-user-vlan 2. port bridge Deleted Features: 1. The SubVLAN in SuperVLAN can be configured to be isolated-vlan
S3610_5510-CMW520-F5315	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. IPv6 Source Guard. 2. DHCPv6 Snooping. 3. ND Snooping. 4. ND Detection. 5. IPv6 PIM DM/SSM/SM. 6. IPv4 IGMP Snooping Group Policy. 7. IPv6 MLD Snooping Group Policy. 8. Y.1731. 9. Setting the MTU of IPv6 packets sent over an interface. 10. IPv6 Multicast VLAN+. 11. The maximum number of neighbors that can be dynamically learned on an interface is configurable. 12. The SubVLAN in SuperVLAN can be configured to be isolated-vlan. 13. Command authorization supports backup method. 14. Ethernet OAM handshake packet transmission interval is configurable. 15. Pasword Control, which refers to a set of functions provided by the local authentication server to control user login passwords, super passwords, and user login status based on predefined policies, includes Minimum password length, Minimum password update interval,Password aging,Early notice on pending password expiration,Login with an expired password,Password history and Login attempt restriction. Deleted Features: 1. Multi-service cooperation QoS mode. 2. The QoS – ISG (IP Source Guard) cooperation. 3. The QoS – VoiceVLAN cooperation.
S3610_5510-CMW520-F5310	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. Packet-filter 2. LACP MAD Deleted Features: None
S3610_5510-CMW520-R5309P02	Changed Hardware Features	New Features: None Deleted Features: None

Version Number	Item	Description
	Changed Software Features	New Features: Super VLAN Deleted Features: None
S3610_5510-CMW520-R5309	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-R5308	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None. Modified Features: 1. DHCP Server supports MCE. 2. DHCP Snooping and DHCP Relay coexist. 3. NDP supported on route-mode port. 4. Maximum OSPF processes changed to 16 in mce-mode. 5. Global policy-mode setting supported, and new command line added: policy mode multi-service-cooperation. Deleted Features: None.
S3610_5510-CMW520-R5306	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. Configure IP address on physical port, and the port is work on route mode. 2. Storm suppression for unicast and multicast traffic. 3. BFD works with OSFP. Deleted Features: None
S3610_5510-CMW520-F5305P06	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. TCP flag based ACL 2. Super password remote authentication and turn to local authentication when unreachable 3. GTS support CBS configure 4. Link-delay 5. IP check with Car and Voice vlan with Car 6. ARP-detection static-bind mode 7. Dynamic VLAN assign with name Deleted Features: None
S3610_5510-CMW520-F5305P02	Changed Hardware Features	New Features: None. Deleted Features: None

Version Number	Item	Description
	Changed Software Features	New Features: 1. Storm constrain 2. RRPP protected-vlan 3. Smart link 4. Port security 5. Connectivity Fault Detection 6. BFD for VRRP 7. Stack Management 8. Track 9. sFlow 10. VLAN Mapping 11. ARP detection 12. ARP snooping 13. System-guard 14. Burst-mode 15. LLDP 16. arp rate-limit 17. GR 18. MFF 19. IP Source Guard related 20. mld-snooping drop-unknown Deleted Features: 1. stp bpdu-transparent-forwarding 2. stp bpdu-tagged Modified Feature: None.
S3610_5510-CMW520-R5303P01	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None
S3610_5510-CMW520-R5303	Changed Hardware Features	New Features: Support new packet buffer chip. Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Feature: The source MAC addresses of some Layer2 protocol's packets are selected based on the outgoing ports, instead of only one MAC address on the whole. These protocols are Cluster, DLDP, HABP, LACP, LLDP, MSTP, NDP, NTDP and GVRP.
S3610_5510-CMW520-F5302P01	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None

Version Number	Item	Description
S3610_5510-CMW520-F5302	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. MCE 2. EAD 3. BFD for static route 4. Enable/disable vlan ingress filter 5. bpdu tunnel related features 6. MAC address mirroring Deleted Features: None
S3610_5510-CMW520-R5301	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. High Memory 2. ESFP 3. RRPP 4. OAM 5. DLDP Deleted Features: None
S3610_5510-CMW520-R0001P02	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: Modify 802.3ad, and does't support Pure Dynamic LACP mode, only support Mode of 'Manual' and 'Static'.
S3610_S5510-CMW520-R0001	Changed Software Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: 1. Switch mode between IPV4 and IPV4-IPV6 2. Anti-Attack for IPV6 Deleted Features: None Modified Features: None
S3610_S5510-CMW520-E0001	Changed Hardware Features	First time
	Changed Software Features	First time

Command Line Updates

Table 6 Command line updates

Version Number	Item	Description
S3610_5510-CMW520-R5319P08	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5319P06	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5319P05	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5319P04	New Commands	The commands related to the new features as following, please refer to the features manual for details: 1. CC/FIPS 2. Disabling password recovery capacity
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-F5319P03	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-F5319P02	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-F5318P02	New Commands	None
	Deleted Commands	None
	Modified Commands	None

Version Number	Item	Description
S3610_5510-CMW520-F5318P01	New Commands	**dhcp-snooping information** [**vlan** *vlan-id*] **sub-option** *sub-option-code* [**string** *user-string&<1-8>*] **undo dhcp-snooping information** [**vlan** *vlan-id*] **sub-option** *sub-option-code*
	Deleted Commands	None
	Modified Commands	• **Command 1:** **dhcp-snooping information format** { **normal** | **private** *private* | **standard** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } **undo dhcp-snooping information format** • **Command 2:** **dhcp-snooping information strategy** { **append**| **drop** | **keep** | **replace** } **undo dhcp-snooping information strategy**
S3610_5510-CMW520-F5317	New Commands	Please refer to Details of Added CLI Commands in CMW520-F5317
	Deleted Commands	None
	Modified Commands	• Old: **port isolate-user-vlan** { **host** | **promiscuous** } • New: **port isolate-user-vlan** { **host** | *isolate-user-vlan-id* **promiscuous** }
S3610_5510-CMW520-F5316	New Commands	Please refer to Details of Added CLI Commands in CMW520-F5316
	Deleted Commands	**Syntax** **isolated-vlan enable** **undo isolated-vlan enable** **View** VLAN view Default Level 2: System level **Parameters** None. **Description** Use the isolated-vlan enable command to enable the sub-VLAN, which in a super-VLAN, isolated-vlan mode. Use the undo isolated-vlan enable command to disable the sub-VLAN, which in a super-VLAN, isolated-vlan mode. By default, isolated-vlan mode is not enabled.
	Modified Commands	None

Version Number	Item	Description
S3610_5510-CMW520-F5315	New Commands	Please refer to Details of Added CLI Commands in CMW520-F5315
	Deleted Commands	**policy mode multi-service-cooperation** **undo policy mode multi-service-cooperation**
	Modified Commands	• Old: **classifier** *tcl-name* **behavior** *behavior-name* [**mode** { **do1q-tag-manipulation** | **ip-source-guard** | **voice-vlan** }] • New: **classifier** *tcl-name* **behavior** *behavior-name* [**mode** **do1q-tag-manipulation**]

Version Number	Item	Description

S3610_5510-CMW520-F5310	New Commands	• **Command 1:**
		Syntax
		packet-filter { *acl-number* | **name** *acl-name* } **inbound**
		undo packet-filter { *acl-number* | **name** *acl-name* } **inbound**
		View
		Ethernet interface view, VLAN interface view
		Parameters
		acl-number: Specifies the number of an ACL, which must be in the following ranges:
		1. 2000 to 2999 for basic IPv4 ACLs
		2. 3000 to 3999 for advanced IPv4 ACLs
		3. 4000 to 4999 for Ethernet frame header ACLs
		name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be named **all** to avoid confusion.
		inbound: Specifies to filter the packets received by the interface.
		Description
		Use the **packet-filter** command to apply an ACL to an interface to filter IPv4 packets or Ethernet frames.
		Use the **undo packet-filter** command to restore the default.
		By default, an interface does not filter packets and Ethernet frames.
		Note that you can apply only one IPv4 ACL or one Ethernet frame header ACL on an interface. To modify the ACL configured on an interface, you need to remove the previous configuration first and then configure a new ACL.
		Examples
		# Apply basic IPv4 ACL 2001 to the inbound direction of interface GigabitEthernet 1/0/1.
		`<Sysname> system-view`
		`[Sysname] interface gigabitethernet 1/0/1`
		`[Sysname-GigabitEtherhet1/0/1] ethernet-frame-filter 2001 inbound`
		# Apply advanced IPv4 ACL 3001 to the inbound direction of VLAN interface 10.
		`<Sysname> system-view`
		`[Sysname] interface Vlan-interface 10`
		`[Sysname-Vlan-interface10] ethernet-frame-filter 3001 inbound`

Version Number	Item	Description

		• **Command 2:**
		Syntax
		packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } **inbound**
		undo packet-filter ipv6 inbound
		View
		Ethernet interface view, VLAN interface view
		Parameters
		acl6-number: Specifies the number of a basic or advanced IPv6 ACL, which must be in the range of 2000 to 3999.
		Name: *acl6-name*: Specifies the name of the basic or advanced IPv6 ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be named **all** to avoid confusion.
		Inbound: Specifies to filter the IPv6 packets received by the interface.
		Description
		Use the **packet-filter ipv6** command to apply a basic or advanced IPv6 ACL to an interface to filter IPv6 packets.
		Use the **undo packet-filter ipv6** command to restore the default.
		By default, an interface does not filter IPv6 packets.
		Note that you can apply only one IPv6 ACL on an interface. To modify the ACL configured on an interface, you need to remove the previous configuration first and then configure a new ACL.
		Examples
		# Apply basic IPv6 ACL 2500 to the inbound direction of interface GigabitEthernet 1/0/1.
		`<Sysname> system-view`
		`[Sysname] interface gigabitethernet 1/0/1`
		`[Sysname-GigabitEthernet1/0/1] packet-filter ipv6 2500 inbound`
		# Apply advanced IPv6 ACL 3000 to the inbound direction of interface VLAN interface 20
		`<Sysname> system-view`
		`[Sysname] interface Vlan-interface 20`
		`[Sysname-Vlan-interface20] packet-filter ipv6 3000 inbound`

	Deleted Commands	None
	Modified Commands	None

Version Number	Item	Description
S3610_5510-CMW520-R5309P02	New Commands	• Add Super Vlan feature: 1. **supervlan** **Syntax** supervlan undo supervlan **View** VLAN view **Parameters** None **Description** Use the supervlan command to configure the current VLAN as a super VLAN. Use the undo supervlan command to remove the super VLAN configuration for the current VLAN. **Examples** # Configure VLAN 2 as a super VLAN. <Sysname> system-view [Sysname] vlan 2 [Sysname-vlan2] supervlan 2. **subvlan** **Syntax** subvlan vlan-list undo subvlan [vlan-list] **View** VLAN view **Parameters** vlan-list: Sub-VLAN list **Description** Use the subvlan command to associate the super VLAN with the specified sub-VLAN(s). The current VLAN is the super VLAN whereas the VLANs specified by the vlan-list parameter are the sub-VLANs. Use the undo subvlan command to remove the association. **Examples** # Associate VLAN 10 (the super VLAN) with VLAN 3, VLAN 4, VLAN 5, and VLAN 9 (the sub-VLANs). <Sysname> system-view [Sysname] vlan 10 [Sysname-vlan10] subvlan 3 to 5 9

Version Number	Item	Description
		3. display supervlan **Syntax** display supervlan [supervlan-id] **View** Any view **Parameters** supervlan-id: Super VLAN ID, in the range of 1 to 4094. **Description** Use the display supervlan command to display the mapping between a super VLAN and sub-VLANs, and the information of these VLANs. Related commands: supervlan, subvlan. **Examples** # Display the mapping between a super VLAN and sub-VLANs. <Sysname> display supervlan 2
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5309	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5308	New Commands	**1. policy mode multi-service-cooperation** **Syntax** [undo] policy mode multi-service-cooperation **View:** System view **Parameter:** None. **Description:** The command used to enable policy-mode 'ip-source-guard' and 'voice-vlan' globally. **Example** <Sysname> system-view [Sysname] policy mode multi-service-cooperation **2. ndp enable** 'ndp enable' command supported under both Layer 3 Ethernet interface view and Layer 2 Ethernet interface view
	Deleted Commands	None
	Modified Commands	None

Version Number	Item	Description
S3610_5510-CMW520-R5306	New Commands	The commands related to the new features as following, please refer to the features manual for details: 1. Configure IP address on physical port, and the port is work on route mode. 2. Storm suppression for unicast and multicast traffic. 3. BFD works with OSFP.
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-F5305P06	New Commands	• Remote authentication for super password 1. Command1: **Syntax** super authentication-mode scheme [local] **View:** System view **Parameter:** scheme: user level change and use HWTACAS authentication. Local: Turn to local authentication if the remote authentication is unreachable **Description:** Command “super authentication-mode” use to configure the authentication mode from low level user change to high level. Command “undo super authentication-mode” use to recover the default configuration. By default, when low level user change to high level the super password of local authentication is used. **Example** [H3C] super authentication-mode scheme local 2. Command2: **Syntax** authentication super hwtacacs-scheme hwtacacs-scheme-name undo authentication super **View** ISP domain view **Parameter:** hwtacacs-scheme hwtacacs-scheme-name: the name of HWTACACS **Description:** authentication super is used for the switching of user level in HWTACACS scheme.

Version Number	Item	Description
		Example System View: return to User View with Ctrl+Z. # configure the switching of user level in HWTACACS for ISP domain aabbcc.net as ht <H3C> system-view System View: return to User View with Ctrl+Z. [H3C] domain aabbcc.net New Domain added. [H3C-isp-aabbcc.net] authentication super hwtacacs-scheme ht • GTS support CBS configure **Syntax** qos gts { any | queue queue-number } cir committed-information-rate [cbs committed-burst-size] undo qos gts { any | queue queue-number } **View** Ethernet port view, port group view **Parameter** any: Performs traffic shaping (TS) for all the packets. queue queue-number: Performs TS for packets in the queue identified by the queue-number argument, in the range of 0 to 7. cir committed-information-rate: Specifies the committed information rate (CIR). The range of the committed-information-rate argument varies by port type as follows: For fast Ethernet port: 650 to 100000 For GigabitEthernet port: 65 to 1000000 Note that the argument must be a multiple of 650. cbs committed-burst-size:Committed burst size (CBS) in bytes, that is, the size of bursty traffic when the actual average rate is not greater than CIR. Range: 4000-16000000. **Description** Use the qos gts command to set GTS parameters and enable GTS for a specific type of traffic or all types of traffic. Use the undo qos gts command to remove GTS parameters for a specific type traffic or all types of traffic. . By default, no GTS parameters are configured for a port.

Version Number	Item	Description
		Example # Perform GTS for all the packets on Ethernet1/0/1 port. Packets with the rate lower than 650 kbps are forwarded normally. The CBS is 1000000.Those with the rate exceeding 650 kbps are dropped. <Sysname> system-view [Sysname] interface Ethernet 1/0/1 [Sysname-Ethernet1/0/1] qos gts any cir 650 cbs 1000000 • Link-delay **Syntax** link-delay *n* **View:** Ethernet port view **Parameter:** *n* <2-10> the seconds for delay. **Description:** Delay for the port UP. **Example** [system -Ethernet1/0/1]link-delay 2 • IP check with Car and Voice vlan with Car **Syntax** classifier classifier-name behavior behavior-name [mode { do1q-tag-manipulation | ip-source-guard | voice-vlan }] undo classifier classifier-name **View** Policy view **Parameter** classifier-name: name of classifier behavior-name: name of behavior mode dot1q-tag-manipulati: For Vlan-mapping mode ip-source-guard: to identify the classifier and behavior is used by IP source guard function. It can use with user-bind and ip check source in ip-source-guard feature, so take the dynamic bind items in dhcp-snooping with CAR policy. And the legal user's traffic can be limited. mode voice-vlan: used together with voice-vlan function. To limit the voice traffic that has voice OUI. **Description** The added new mode is use to apply CAR qos policy to dynamic users. The mode ip-source-guard use to apply CAR with Ip check source or user bind, and limit the traffic of legal users. Such as: enable dhcp-snooping and ip check source, then hope to limit the traffic of the users who apply the IP address legally. You can configure mode ip-source-guard CAR policy on the user side ports, so the user that applies IP address will be affected with CAR policy automatically.

Version Number	Item	Description
		The mode voice-vlan used together with voice-vlan function. To limit the voice traffic that has voice OUI. *Note:* *the classifier must be defined as if-match any* *mode dot1q-tag-manipulation and ip-source-guard cannot be defined in the same policy* *The policy should be applied on ports first, and then the ip source guard or voice vlan functions, so that the function can take effect.* **Example** Using dhcp-snooping and ip check source function and when the user applied IP address by DHCP, then use the CAR qos policy to limit the traffic of the user within 10Mbps bandwidth. Using user-bind to limit the bandwidth of user with IP: 1.1.1.1, MAC: 0000-0000-0002 to 10Mbps. #create qos car policy(can also use aggregative CAR if all the users sharing the same bandwidth): [system]traffic classifier cl [system-classifier-car]if-match any [system]traffic behavior be [system-behavior-be]car cir 10000 [system]qos policy ipcheck [system-qospolicy-ipcheck]classifier cl behavior be **mode ip-source-guard** #apply the policy on port [system]interface Ethernet 1/1/1 [system-Ethernet1/1/1]qos apply policy ipcheck inbound #enable ip check source: <SwitchA> system-view [SwitchA] interface ethernet1/0/1 [SwitchA-Ethernet1/0/1] ip check source ip-address mac-address [SwitchA-Ethernet1/0/1] quit [SwitchA] dhcp-snooping #enable user-bind [SwitchA-Ethernet1/0/1] user-bind ip-address 1.1.1.1 mac-address 0-0-2

Version Number	Item	Description
		• ARP-detection static-bind mode 1. Command 1: **Syntax** arp detection mode { dhcp-snooping | dot1x | static-bind } undo arp detection mode [dhcp-snooping | dot1x | static-bind] **View** System view **Parameters** dhcp-snooping: Implements ARP attack detection based on DHCP snooping entries. This mode is mainly used to prevent source address spoofing attacks. dot1x: Implements ARP attack detection based on 802.1X security entries. This mode is mainly used to prevent source address spoofing attacks. static-bind: Implements ARP attack detection based on static IP-to-MAC binding entries. This mode is mainly used to prevent gateway spoofing attacks. **Description** Use the arp detection mode command to specify an ARP attack detection mode. Use the undo arp detection mode command to cancel the specified ARP detection mode or all ARP detection modes. If all detection modes are cancelled, ARP detection is not performed. By default, no ARP detection mode is specified, that is, ARP detection based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings is not enabled. Note that: You can specify the three modes at the same time. In dot1x mode: if an entry with matching source IP and MAC addresses, port index, and VLAN ID is found, the ARP packet is considered valid and can pass the detection; If an entry with no matching IP address but with a matching OUI MAC address is found, the ARP packet is considered valid and can pass the detection; if otherwise, the ARP packet is discarded. In static-bind mode: If an entry with a matching IP address but with a different MAC address is found, the ARP packet is considered invalid and discarded; if an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection; if no match is found, the ARP packet is considered valid and can pass the detection. If no ARP detection mode is specified in the undo arp detection mode command, all configured ARP detection modes are disabled.

Version Number	Item	Description
		Examples # Enable ARP detection based on DHCP snooping entries. <Sysname> system-view [Sysname] arp detection mode dhcp-snooping 2. Command 2: **Syntax** arp detection static-bind ip-address mac-address undo arp detection static-bind [ip-address] **View** System view **Parameters** ip-address: IP address of the static binding. mac-address: MAC address of the static binding, in the format of H-H-H. **Description** Use the arp detection static-bind command to configure a static IP-to-MAC binding. Use the undo arp detection static-bind command to remove the configure static binding. By default, no static IP-to-MAC binding is configured. With ARP detection based on static IP-to-MAC bindings configured, the device, upon receiving an ARP packet from an ARP trusted/untrusted port, compares the source IP and MAC addresses of the ARP packet against the static IP-to-MAC bindings. If an entry with a matching IP address but different MAC address is found, the ARP packet is considered invalid and discarded. If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection. If no match is found, the ARP packet is considered valid and can pass the detection. Note that: If no IP address is specified in the undo arp detection static-bind command, all configured static IP-to-MAC bindings are removed. **Examples** # Configure a static IP-to-MAC binding. <Sysname> system-view [Sysname] arp detection static-bind 192.168.1.2 2-1-201

Version Number	Item	Description
		• Dynamic VLAN assign with name **Syntax** name string **View:** VLAN view **Parameter:** *string*: the name of the VLAN. Length 1-32 characters. **Description:** The command use to configure the name of the VLAN. **Example** [system-vlan2] name hello
	Deleted Commands	None
	Modified Commands	TCP flag based ACL The ACL in the range 3000-3999 modify the key word after TCP from “established” to every TCP flag, such as: ack, fin, psh, rst, syn, urg.
S3610_5510-CMW520-F5305P02	New Commands	Burst-mode: System-view: burst-mode enable Description: Enhance the burst flow buffering ability on the device. The commands related to the new features as following, please refer to the features manual for details: 1. Storm constrain 2. RRPP protected-vlan 3. Smart link 4. Port security 5. Connectivity Fault Detection 6. BFD for VRRP 7. Stack Management 8. Track 9. sFlow 10. VLAN Mapping 11. ARP detection 12. ARP snooping 13. System-guard 14. IP Source Guard related 15. LLDP 16. arp rate-limit 17. GR 18. MFF 19. mld-snooping drop unknown
	Deleted Commands	1. stp bpdu-transparent-forwarding 2. stp bpdu-tagged 3. bpdu-tunnel dot1q enable

Version Number	Item	Description
	Modified Commands	4. Voice VLAN The configuration of Voice VLAN id has been moved from the system view to port view. 5. traffic classifier Command "If-match dot1p" is replaced by commands: if-match customer-dot1p if-match service-dot1p 6. NQA command "nqa STRING<1-32>" is replaced by : nqa agent | entry | schedule | server 7. Aggregation command: Modify the command "link-aggregation" to "interface Bridge-Aggregation" 8. level Under Local-User view, command "level" is replaced by "authorization-attribute level"
S3610_5510-CMW520-R5303P01	New Commands	None
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5303	New Commands	**vlan-check disable** Please refer to Command Manual.
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-F5302P01	New Commands	None
	Deleted Commands	None
	Modified Commands	None

Version Number	Item	Description
S3610_5510-CMW520-F5302	New Commands	1. Added new feature MCE refer to 'H3C S3610 Series Ethernet Switches Operation Manual' 2. Added new feature EAD refer to '802.1X Operation Manual' 3. Added new feature BFD for static route refer to 'H3C S3610 Series Ethernet Switches Operation Manual' 4. Add new feature Enable/disable vlan ingress filter Add new command in port view : [undo] vlan-check ignored 5. Added new feature bpdu tunnel related features 6. Added new command in port view : 'stp bpdu-transparent-forwarding' 7. Added new command in port view : 'stp bpdu-tagged' 8. Add new command in system view : 'stp bpdu-transparent-forwarding vlan' 9. Add new command in system view: 'stp interface interface_list bpdu-tagged' 10. Added new feature MAC address mirroring 11. Add new command in port view: mac- mirroring < index > src-vlan < source_vlan_list > dest-vlan < destination_vlan_id > mac- mirroring < index > src-vlan < source_vlan_id > dest-vlan < destination_vlan_list > undo mac- mirroring { < index > }
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R5301	New Commands	1. Add new feature ESFP refer to <H3C S3610 Series Ethernet Switches Operation Manual> 2. Add High memory refer to <H3C S3610 Series Ethernet Switches Operation Manual> 3. Add new feature RRPP refer to <H3C S3610 Series Ethernet Switches Operation Manual> 4. Add new feature OAM refer to <H3C S3610 Series Ethernet Switches Operation Manual> 5. Add new feature DLDP refer to <H3C S3610 Series Ethernet Switches Operation Manual>

Version Number	Item	Description
	Deleted Commands	None
	Modified Commands	None
S3610_5510-CMW520-R0001P02	New Commands	None
	Deleted Commands	Deleted Command: 1. [H3C-GigabitEthernet1/0/1]lacp enable 2. [H3C-GigabitEthernet1/0/1]undo lacp enable Specification: the Mode of 'Static' also run LACP, and can replace Pure Dynamic LACP mode.
	Modified Commands	None
S3610_S5510-CMW520-R0001	New Commands	1. command 1 [H3C]switch-mode { default | dual-ipv4-ipv6 } , Usage of this command refer to<H3C S3610&S5510 Series Ethernet Switches Command Manual -Release 0001> 2. command 2 [H3C]dis switch-mode display the current and the next reboot mode ,
	Deleted Commands	None.
	Modified Commands	None
S3610_S5510-CMW520-E0001	New Commands	First time.
	Deleted Commands	First time.
	Modified Commands	First time.

MIB Updates

Table 7 MIB Updates

Version Number	Item	MIB File Name	Module Name	Description
S3610_5510-CMW520-R5319P08	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-R5319P06	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-R5319P05	New	None	None	None
	Modified	None	None	None

S3610_5510-CMW520-R5319P04	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-F5319P03	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-F5319P02	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-F5318P02	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-F5318P01	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-F5317	New	None	None	None
	Modified	None	None	None
S3610_5510-CMW520-F5315	New	rfc4293-ip-mib.mib	IP-MIB	Supports RFC4293
	Modified	None	None	None
S3610_5510-CMW520-F5305P02	New	None	None	None
	Modified	MIB style	None	Change from compatible to new style by default

Configuration Changes

Operation Changes in CMW520-R5319P08

None

Operation Changes in CMW520-R5319P06

None

Operation Changes in CMW520-R5319P05

None

Operation Changes in CMW520-R5319P04

None

Operation Changes in CMW520-F5319P03

Backup the configuration file for old version software:

If a save operation is performed on a switch where a software version of F5319P03 or later is running and the version number in the current startup configuration file is lower than F5318P02 (not include F5318P02), the system first backs up the startup configuration file and then saves the current configuration. For example, suppose the startup configuration file is a.cfg. When a save operation is performed, the system first backs up a.cfg into _a_bak.cfg and then saves the current configuration into a.cfg.

Operation Changes in CMW520-F5319P02

Disable all the TCP/UDP port by default (For example: TCP ports including 23/7547, UDP ports including 68/1812/3318/3799).

Disable HTTP service by default. In earlier versions, HTTP is enabled by default. In this version, HTTP is disabled by default.To enable HTTP; use the “ip http enable” command.

Disable telnet server by default. In earlier versions, telnet server is enabled by default. In this version, telnet server is disabled by default.To enable telnet server, use the “telnet server enable” command.

Operation Changes in CMW520-F5318P02

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

Operation Changes in CMW520-F5318P01

None

Operation Changes in CMW520-F5317

As configuring the isolate-user-VLAN type of a port as promiscuous, the isolate-user-VLAN to which the port belongs must be provided.

Operation Changes in CMW520-F5316

By default, LLDP is enabled.

Operation Changes in CMW520-F5315

The maximum number of instances that MSTP supports has been increased to 32.

The maximum number of backup groups that VRRP supports has been increased to 20.

The maximum number of backup groups that VRRPv6 supports has been increased to 20.

The range of minimum interval for transmitting BFD control packets has been changed to 100~1000ms.

The range of minimum interval for receiving BFD control packets has been changed to 100~1000ms.

The maximum number of OSPF processes has been increased to 16 in MCE mode.

The range of BGP AS identifier has been changed to 1~4294967295.

The WEB managment UI has changed to new style, and the ‘Jumbo-frame configuration’ was removed.

Operation Changes in CMW520-F5305P02

The command “ip redirects enable” is disable by default.

The command “ip unreachables enable” is disable by default.

The NDP MAC changes to 0180-C200-000A.

Operation Changes in CMW520-R0001

Add Switch-mode command, Reboot device afer Switch Work mode.

Move command **‘qinq ethernet-type’** to port view.

Open Problems and Workarounds

D08420

- First Found-in Version: CMW520-R0001
- Description: These packets were forwarded if the packets’ destination ip address is Class-E (240.0.0.0---255.255.255.255)
- Avoidance: Using ACL to filter these packets.

LSD05495

- First Found-in Version: CMW520-R0001
- Description: Ping is failed between link local address configured in the tunnel interface. Or Routing Protocol is ineffective in the tunnel interface.
- Avoidance: Configuring expedited termination tunnel.

LSD67705

- First Found-in Version: CMW520- F5318P01
- Description: In this version of code, the password encryption within configuration files has been enhanced and cannot be interpreted by earlier revisions of the agent code. This means that if a unit is downgraded to earlier code, it may no longer be possible to login and manage the device.
- Avoidance:
  - Before upgrading to the new code, it is necessary to ensure password control is disabled. Execute the “*undo password-control enable*” and then save this configuration file as a backup in case you need to downgrade the software again. If it is later necessary to downgrade to earlier software, force the switch to use this backup configuration file by executing a *”startup saved-configuration (filename)”* command before rebooting to the old code. Then, after the code has been downgraded, the device can be logged in from the console or by Telnet, but not SSH. The SSH authentication details will need to be reset.
  - If no backup configuration has been saved but it is still possible to access the device management via some method while running the old code (e.g. Console, Telnet or SSH), then you can redefine all the device management passwords as required.
  - If after a downgrade it is impossible to login to the device via any method, then there are two ways to recover the switch:

- From the BOOT menu, set the new code to run again and reboot the device. Disable Telnet authentication:
  User-interface vty 0 4
  Authentication mode none
  Then save the configuration and downgrade the code again, login via Telnet and reset all the passwords as required.

- From the BOOT menu. On boot-up, use Ctrl+B to enter the Boot menu and then force the unit to use the factory default configuration (bypassing the user configuration). The unit will then need to be fully reconfigured.

LSD074159

- First Found-in Version: CMW520-R5319P04
- Description: The switch runs FIPS mode, when the user login the switch first time use web there is no dialog box suggests the user to modify password.
- Avoidance: None.

List of Resolved Problems

Resolved Problems in CMW520-R5319P08

201402190175

- First Found-in Version: CMW520-R5319P04
- Description: Fail to save configuration or load file to the flash.
- Condition: Some devices run a long time, and the flash chip worn out.

201406120024

- First Found-in Version: CMW520-R5319P06
- Description: CVE-2014-0224.
- Condition: When Open SSL Server or Client is used.

Resolved Problems in CMW520-R5319P06

LSD074587

- First Found-in Version: CMW520-R5319P05
- Description: Device could not handle invalid SNMP packet and resulted in an exception.
- Condition: Device received an invalid SNMP packet with overlong OID.

LSD074729

- First Found-in Version: CMW520-R5319P05
- Description: Device could not handle SSH packet which had many special characters and resulted in an exception.
- Condition: Device received a SSH packet which had many 0x07 as control-character.

LSD074587

- First Found-in Version: CMW520-R5319P05
- Description: Device could not handle invalid SNMP packet and resulted in an exception.
- Condition: Device received an invalid SNMP packet which had an oversize ContextName field.

Resolved Problems in CMW520-R5319P05

LSD074316

- First Found-in Version: CMW520-R5319P04
- Condition: When system receives DHCP packet which contains abnormal option 82 field.
- Description: The switch experiences unexpected reboot or hung because of fatal error.

Resolved Problems in CMW520-R5319P04

None

Resolved Problems in CMW520-F5319P03

LSD074058

- First Found-in Version: CMW520-F5319P02
- Condition: The switch runs on the F5318P02 or F5319P02 version. When the startup configuration file exists, and then execute save operation to overwrite the old startup configuration file.
- Description: The switch will reboot in very low probability.

Resolved Problems in CMW520-F5319P02

LSD073645

- First Found-in Version: CMW520-F5318P01
- Condition: The switch runtime more than 497 days.
- Description: The CPU usage is high when some ports up/down.

LSD072427

- First Found-in Version: CMW520-F5318P01
- Condition: The VLAN-interface configured primary IP address and sub IP address, and these IP addresses belong to the range of rip network both. Then delete the sub IP address only.
- Description: The VLAN-interface cannot receive the RIP protocol packets, and cannot learn RIP routes.

Resolved Problems in CMW520-F5318P02

LSD073067

- First Found-in Version: CMW520-F5318P01

- 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 CMW520-F5318P01

LSD65740

- First Found-in Version: CMW520-F5317
- Condition: Switch runs SNMP, and the net manager software get the MIB of dot3StatsTable.
- Description: The switch runs abnormally.

LSD65861

- First Found-in Version: CMW520-F5317
- Condition: The switch-mode is dual-ipv4-ipv6, and executes the command of “display diagnosis”.
- Description: The switch runs abnormally.

LSD60648

- First Found-in Version: CMW520-R5309
- Condition: Configures redirect to next-hop in global.
- Description: When the ARP of the next-hop added or deleted or changed, the action of the ACL can’t change accordingly.

ZDD03980

- First Found-in Version: CMW520-F5317
- Condition: In some conditions, BGP issues routes aggregation in private network without RT attribute.
- Description: The neighbor devices can’t learn the routes aggregation.

ZDD04002

- First Found-in Version: CMW520-F5317
- Condition: None.
- Description: The implement of dot1qVlanStaticUntaggedPorts is not accord with RFC4363.

ZDD03991

- First Found-in Version: CMW520-F5317
- Condition: The user’s parameters on Radius server contain callback-number witch length equal to 63 bytes.
- Description: Some data in memory of the switch will be destroyed.

Resolved Problems in CMW520-F5317

LSD50990

- First Found-in Version: CMW520-F5316

- Condition: Configures port bridge enable on the active combo port, and switch active combo port.
- Description: The current active combo port works in port bridge mode.

LSD52934

- First Found-in Version: CMW520-F5315
- Condition: Configure Multicast-VLAN and enable igmp-snooping and the Multicast-VLAN function works mormally.The VLAN which configured as multicast-vlan was deleted and then created again,and configured as Multicast-VLAN(igmp-snooping enabled,subvlan configured).
- Description: The host cannot receive the stream required.

LSD52435

- First Found-in Version: CMW520-R5309
- Condition: Configure IPv6 address in interface, and there are several '0' s typed before the really prefix length, for example: 'ipv6 address 2008::100/000…064', there are 480 '0's before '64'.
- Description: The switch may reboot abnormally.

LSD52437

- First Found-in Version: CMW520-R5303
- Condition: LLDP is enabled and the speed of one port is configured as non-autonegotiation.
- Description: The auto-negotiation state of LLDP information of the port advertised by the LLDP function is wrong.

LSD52440

- First Found-in Version: CMW520-R5303
- Condition: LLDP is enabled and VLAN name is configured.
- Description: VLAN name in the LLDP information is wrong.

LSD52455

- First Found-in Version: CMW520-R5303
- Condition: 'debugging lldp packet' is enabled, and the switch receives LLDP packet which carry a ChassisId longer than the maximum defined in the standard.
- Description: The switch may reboot abnormally.

LSD53662

- First Found-in Version: CMW520-R5303
- Condition: Display port-security mac-address security.
- Description: The information, 'No Multicast Mac addresses found.' may confuse the operator.

LSD55154

- First Found-in Version: CMW520-R5309
- Condition: The switch is running SSH Server service and suffers SSH login attacks such as user name guess or password guess.
- Description: The switch may reboot abnormally.

LSD56601

- First Found-in Version: CMW520-R5315
- Condition: The system is running in Compatible mib-style.
- Description: The panel of the switch shown in web page is incorrect.

ZDD03542

- First Found-in Version: CMW520-R5309
- Condition: Enable DHCP Relay function, and the host moves to another VLAN after obtains a IP address.
- Description: The temporary dhcp-security items can not been deleted.

ZDD03650

- First Found-in Version: CMW520-R5306
- Condition: Configure the MAS-IP in of HWTACACS or RADIUS.
- Description: NAS-IP cannot accepts the IP address that its least significant octet is 255(Class A IP address 18.1.1.255, etc.).

ZDD03251

- First Found-in Version: CMW520-R5309
- Condition: The trap target host is configured after reboot.
- Description: The switch sends 'coldStart' (its OID is 1.3.6.1.6.3.1.1.5.1) trap message wrongly.

ZDD03328

- First Found-in Version: CMW520-R5309
- Condition: An interface uses DHCP client function to obtain an IP address from the DHCP server. The DHCP server sends the offer packets without 'end-option' field.
- Description: The interface can't obtain an IP address.
-

ZDD03047

- First Found-in Version: CMW520-R5309
- Condition: The device is running NDP and NTDP protocols and has collected the neighbor's infotmation. The 'ntdp explore' command is excuted continually to collect the topology infomation manually, and the neighbor's information updates during this collecting process.
- Description: The switch may reboot abnormally.

Resolved Problems in CMW520-F5316

LSD44598

- First Found-in Version: CMW520-R5303
- Condition: QinQ functions were configured by modifying the configuration file manually and the 'qinq vid' configured in disorder. Then configures a new 'qinq vid'.

- Description: The switch reboots.

LSD46541

- First Found-in Version: CMW520-F5315
- Condition: Update the software by Web manager.
- Description: The operation will fail.

LSD46551

- First Found-in Version: CMW520-F5315
- Condition: When STP is enabled and link aggregation is configured at the same time on the switch.
- Description: The STP state of the member port of the link aggregation in hardware probably is not consistent with that in software. This may cause loops in the network.

LSD46576

- First Found-in Version: CMW520-F5315
- Condition: Add and delete a lot of ND entries repeatedly.
- Description: The memory leak occurs.

LSD46580

- First Found-in Version: CMW520-F5315
- Condition: Create tunnel interface and configure the loopback port by the command “service-loopback-group”. Then save the configuration and reboot the switch.
- Description: After the switch reboot, the tunnel interface couldn’t UP.

LSD46703

- First Found-in Version: CMW520-F5315
- Condition: If there are a lot of IPv6 data packets sent to the switch, and the packet’s target is the switch.
- Description: The status of OSPFv3 could not keep stable.

LSD46916

- First Found-in Version: CMW520-F5315
- Condition: Create two VLAN interfaces on the switch, and only one of them configures IP address. Then shutdown the VLAN interface which not configure IP address.
- Description: The switch CPU couldn’t receive the broadcast ARP request packets.

LSD46733

- First Found-in Version: CMW520-F5315
- Condition: Add and delete a lot of route entries repeatedly.
- Description: Can’t establish OSPF neighbor probably.

LSD46742

- First Found-in Version: CMW520-F5315

- Condition: The switch runs IPv6 multicast routing, add and delete a lot of IPv6 route entries repeatedly.
- Description: Can't create IPv6 multicast route entry probably.

LSD48385

- First Found-in Version: CMW520-F5315
- Condition: Creates link-aggregation group, and the members had Down/Up or quitted/added the group.
- Description: The traffic output port of the hash result maybe change.

LSD48332

- First Found-in Version: CMW520-F5315
- Condition: Some SPF ports insert optic module, and the ports are UP.
- Description: Display the alarm information of the modules, print Rx Los alarming.

LSD47252

- First Found-in Version: CMW520-F5315
- Condition: The switch disables LLDP globally.
- Description: The LLDP packets can be transmitting by the switch.

LSD46752

- First Found-in Version: CMW520-F5315
- Condition: Enable MFF on VLAN.
- Description: The multicast traffic will be dropped.

ZDD03047

- First Found-in Version: CMW520-F5315
- Condition: The switch enables NTDP and executes the command" ntdp explore" repeatedly.
- Description: The switch reboots.

LSD50680

- First Found-in Version: CMW520-F5315
- Condition: The switch enables IPv6, creates VLAN interface and configures IPv6 address. The status of the VLAN interface is UP.
- Description: The solicited node packets can't be sent to CPU.

LSD50181

- First Found-in Version: CMW520-F5315
- Condition: Configures packet-filter rules on the VLAN interface which runs VRRP.
- Description: The routing packet which destination MAC is VRRP route MAC can't match the packet-filter rules.

LSD50456

- First Found-in Version: CMW520-F5315
- Condition: When a lot of MAC-authentication users logon, and the port which configures MAC-authentication UP/DOWN repeatedly.
- Description: The switch reboots.

Resolved Problems in CMW520-F5315

LSD43634

- First Found-in Version: CMW520-R5309
- Condition: The switch runs the DHCP relay security function, and some clients released the IP addresses abnormally.
- Description: Some clients couldn't apply IP address anymore.

Resolved Problems in CMW520-F5310

LSD34593

- First Found-in Version: CMW520-R5306
- Condition: In the "Tunnel interface" view.
- Description: There have some command lines of Qos which cannot be supported.

LSD36615

- First Found-in Version: CMW520-R5309P02
- Condition: The SFP slot inserts the optic module 3CSFP9-81 or 3CSFP9-82.
- Description: The 100M SFP slot with the module will alternate between UP and DOWN repeatedly; the 1000M SFP slot with the module can't change to UP.

LSD40748

- First Found-in Version: CMW520-R5309P02
- Condition: The duplex status of the port is autonegotiation.
- Description: When the network manage software get the duplex status of the port used MIB, the result will be "Unknown".

ZDD02344

- First Found-in Version: CMW520-R5309P02
- Condition: The switch runs LLDP, the VLAN hasn't configure IP address, and the VLAN ID is the minimum that the port permits pass.
- Description: The Management address in the LLDP packets is 127.0.0.1.

ZDD02245

- First Found-in Version: CMW520-R5309P02

- Condition: Login on the web used https, and the used certificate is link form or equal or more than level 3.
- Description: The switch reboots.

ZDD02151

- First Found-in Version: CMW520-R5309P02
- Condition: Switch work as Telnet client or server. Input non-english character after login.
- Description: Possible unexpected logout.

ZDD02141

- First Found-in Version: CMW520-R5309P02
- Condition: The switch link with stack devices trough LACP.
- Description: The stack devices could not detect stack split rapidly.

Resolved Problems in CMW520-R5309P02

LSD36815

- First Found-in Version: CMW520-R5309
- Condition: The switch is running Ipv6 and OSPFV3 with another Ipv6 device, add VLAN ACL by command “qos vlan-policy”.
- Description: The OSPFV3 neighbor changes to be down.

LSD38325

- First Found-in Version: CMW520-R5309
- Condition: Add time-range based ACL on any of the later 16 ports of S5510 switch.
- Description: The ACL cannot be deleted when the time expires.

ZDD02045

- First Found-in Version: CMW520-R5309
- Condition: Enable SNMP function on devices.
- Description: Sometimes different devices have the same snmp local-engineid, which cause the devices not manageable by SNMP manager.

LSD38527

- First Found-in Version: CMW520-R5309
- Condition: Create Bridge-Aggregation and add ports to it, then add Aggregation group to a VLAN in VLAN view.
- Description: The member ports are not added to the VLAN accordingly.

LSD38439

- First Found-in Version: CMW520-R5309
- Condition: Enable LLDP on the device and connect it to some VoIP Phones.
- Description: The LLDP neighbor may not establish successfully.

LSD40506

- First Found-in Version: CMW520-R5309
- Condition: Define the ACL rule to set one bit of TCP flag, for example, ACK, without caring the other bits.
- Description: The flow can only be matched by this ACL when its relevant non-setting bits of TCP flag are zero.

Resolved Problems in CMW520-R5309

LSD37888

- First Found-in Version: CMW520-R5308
- Condition: The device works in low temperature environment.
- Description: Few CRC error packets occur on few devices.

Resolved Problems in CMW520-R5308

LSD32811

- First Found-in Version: CMW520-R5303
- Condition: Power failed while deleting a file.
- Description: The switch cannot start up due to a lost or damaged boot-loader file.

LSD35029

- First Found-in Version: CMW520-R5306
- Condition: To switch link-mode of a port to route-mode.
- Description: NDP is not supported under the port-interface view.

LSD35505

- First Found-in Version: CMW520-R5306
- Condition: A policy is applied to VLAN, which permits ICMP packets, permits special source IP address and destination IP address TCP packets, and denies other IP stream.
- Description: ICMP packets are permitted, but Telnet stream is denied.

LSD35657

- First Found-in Version: CMW520-R5306
- Condition: DHCP Snooping and VLAN mapping configured on the device.
- Description: VLAN mapping cannot work.

LSD36612

- First Found-in Version: CMW520-R5306
- Condition: ping the IP address of the device from a PC's virtual LACP link-aggregation interface which support Marker protocol described in IEEE 802.3ad.
- Description: the round-trip time is too long.

LSD36654

- First Found-in Version: CMW520-R5303
- Condition: down-grade application software from version newer than R5303 (included) to the one older than R5303.
- Description: down-grade failed.

LSD36699

- First Found-in Version: CMW520-R5306
- Condition: DHCP Relay enabled.
- Description: DHCP Client such as Ms Windows Vista OS, which send “DHCP Inform Message” (option 53), cannot get an IP address.

LSD36871

- First Found-in Version: CMW520-R5306
- Condition: Member port of a link-aggregation is up; shutdown the remote port or pull out the network cable.
- Description: The member port changes to inactive state, but the link state keeps up.

Resolved Problems in CMW520-R5306

None

Resolved Problems in CMW520-F5305P06

LSD29079

- First Found-in Version: VRP520-F5305P02
- Condition: Use bootrom135 or bootrom137 with the F5305P02 software.
- Description: The switch reboot repeatedly.

LSD31267

- First Found-in Version: VRP520-F5305P02
- Condition: The switch has lot of ECMP routes, and there have lot of traffic that need IP route.
- Description: CPU rate is high.

LSD31725

- First Found-in Version: VRP520-F5305P02
- Condition: Configure qos policy on a port, and the policy is null.
- Description: The configuration can’t be cancel.

LSD32146

- First Found-in Version: VRP520-F5305P02

- Condition: Configure selective QinQ mapping on a port, and then remove the mapping with the command “undo raw-vlan-id inbound”. Configure another mapping on the port, and then configure the first mapping again.
- Description: The second mapping is inactive.

LSD32434

- First Found-in Version: VRP520-F5305P02
- Condition: The switch work with CAMS, and pass the authentication.
- Description: The accounting network manages software can’t get the user’s IP address.

LSD32577

- First Found-in Version: VRP520-F5305P02
- Condition: Insert specific 100M SFP module into 100M SFP slot.
- Description: The switch can’t recognize the type of ESFP module, and display “UNKNOWN_SFP”.

Resolved Problems in CMW520-F5305P02

LSD27375

- First Found-in Version: CMW520-R5303
- Condition: Using SNMP MIB tool to walk the node “ospfExtLsdbAdvertisement”.
- Description: The query will be timeout, and the CPU of the switch will raise high for a while.

LSD26450

- First Found-in Version: CMW520-R5301
- Condition: Adding a static route entry by “ip route-static” to the switch. If the AND operation of Destination IP address and it’s mask is 0.0.0.0, but the mask itself is not all 0s, for example:
- ip route-static 120.1.1.2 1 10.1.1.2
- Description: The IP flow matching this subnet will be forwarded by CPU, instead of the switch chip.

LSD27579

- First Found-in Version: CMW520-R5303
- Condition: There is no configuration on the switch except “telnet server enable” which is used for the Cluster management. After booting up, connect to the switch from a Cluster Command device, and create VLANs but do nothing else in the VLAN view; Or, There is no configuration on the switch. After booting up, configure VLAN 1 so as to be Telnet-ed. Then telnet to this switch from another device, and create VLANs, but do nothing else in the VLAN view.
- Description: If using command “display current-configuration”, these new VLANs information will not be displayed as expected. If you save the configuration and reboot the switch, you will find that all these VLANs (except VLAN 1) related information is lost.

LSD27860

- First Found-in Version: CMW520-R5301
- Condition: Plug the ESFP module into the device.

- Description: The CPU usage rate may rise.

LSD27408

- First Found-in Version: CMW520-R5303
- Condition: Configure the switch as a Cluster command device. At cluster view, configure “build” and “undo build” frequently.
- Description: The system memory leaks gradually.

LSD00015

- First Found-in Version:CMW520-R5303
- Condition: When using command “snmp-agent target-host trap”.
- Description: It is unable to configure IPv6 target host.

LSD26273

- First Found-in Version:CMW520-R5303
- Condition: For S3610-52M only, plug the 1000BASE-T SFP module to the combo SFP port, shut down the port, and the port is connected to another device. Reboot the S3610-52M device.
- Description: After the rebooting, the port of the opposite device is still in Link-up state.

LSD21330

- First Found-in Version:CMW520-R5303
- Condition: Enable Loopback detection and the QinQ function on the port where there is network loop existing.
- Description: The Loopback detection cannot detect all the VLANs of the loop.

LSD26473

- First Found-in Version:CMW520-R5303
- Condition: Enable both the Basic QinQ and selective QinQ on the port, for example:

```
#
interface Ethernet1/0/1
port access vlan 800
qinq enable
qinq vid 900
raw-vlan-id inbound all
#
```

Send the packets with the VLAN tag priority other than zero to this port.

- Description: The packets are not added with the service VLAN 900, but VLAN 800.

LSD25635

- First Found-in Version:CMW520-R5303
- Condition: Using IPv6 protocol, and the network SW2------SW1------PC. SW1 and SW2 can communicate with IPv6. SW1 is configured with IPv6 Tunnel to connect to PC. When there’s no SW2’s IPv6 ND entry on SW1.
- Description: The PC cannot ping SW2.

Resolved Problems in CMW520-R5303P01

None

Resolved Problems in CMW520-R5303

LSD23047

- First Found-in Version: CMW520-F5302P01
- Condition: Enable VRRP function on the device, turn on the “debug tcp” command, and perform the NQA test.
- Description: The VRRP status may be unstable.

HSD28837

- First Found-in Version: CMW520-F5302P01
- Condition: The two IPv6 hosts connect to the switch in different subnet. One of the hosts establishes the ISATAP tunnel with the switch, and PING the other host with the packets larger than 1432 bytes.
- Description: The PING will fail.

LSD24388

- First Found-in Version: CMW520-F5302P01
- Condition: Enable EAD quick deployment on the switch, and enable DOT1X on one port, and then add a static MAC entry for the PC that connected to this port.
- Description: When log on to the switch through WEB page from this PC, the page is redirected to the CAMS server.

ZDD01560

- First Found-in Version: CMW520-F5302P01
- Condition: Enable DHCP-snooping on the switch. The DHCP client will get IP address from a DHCP server through this switch.
- Description: The DHCP client cannot get “Service Location” info by the command “slpinfo /d”.

ZDD01566

- First Found-in Version: CMW520-F5302P01
- Condition: Enable OSPF on the switch. Add a static route whose next hop is in the range of subnet that configured by OSPF “network” command. Import the static routes to OSPF, and shut/undo shut the relevant VLAN interface continuously.
- Description: The system task may fall into exception.

LSD24384

- First Found-in Version: CMW520-F5302P01
- Condition: Enable EAD quick deployment on the switch. Configure some parameters like “Free-ip”.
- Description: Some of the “EAD quick deploy configuration” information on management WEB page will lose.

Resolved Problems in CMW520-F5302P01

LSD20766

- First Found-in Version: CMW520-F5302
- Condition: Create a few of IP Subnet-based vlan on a port and then assign a IP address for each IP Subnet-based vlan interface.
- Description: The IP Subnet-based vlan interfaces can't ping each other.

LSD21908

- First Found-in Version: CMW520-F5302
- Condition: Area 0 and NSSA area exist at the same time in the switch. Configuring no network in area 0.
- Description: The switch is selected as ARB router mistakenly, and product wrong ABR route to the switch in other router in the NSSA area.

ZDD01488

- First Found-in Version: CMW520-F5302
- Condition: Receiving igmp packets with length parameter is 0.
- Description: The method of dealing with the igmp packets is improper, possible the device will occur infinite loop and reboot.

ZDD01486

- First Found-in Version: CMW520-F5302
- Condition: There is lack of user tasks in using telnet. It cause failing on starting telnet function.
- Description: Failed to start telnet function again. After stopped telnet function.

Resolved Problems in CMW520-F5302

LSD20368

- First Found-in Version:CMW520-R5301
- Condition: 'burst traffic' command adds port group configuration mode.
- Description: 'burst traffic' command adds port group configuration mode.

Resolved Problems in CMW520-R5301

LSD11730

- First Found-in Version: CMW520-R0001
- Condition: Enable layer 2 multicast or disenable layer 2 multicast.
- Description: Received unknown Layer 2 multicast date packet broadcast in vlan.

LSD15695

- First Found-in Version: CMW520-R0001P02

- Condition: A device get a IP address from DHCP server, and the IP address distributed by DHCP server belong to a network section and TFTP server belong to another network section . Then the device get configuration file from TFTP server.
- Description: The device can't get configuration file from TFTP server.

LSD15851

- First Found-in Version: CMW520-R0001P02
- Condition: Configure voice vlan and security on a port and receiving L2 data stream with voice vlan's tag and variation mac on the port. Then "shutdown" and "undo shutdown" the port.
- Description: Some mac entries exist in software table but not exist in hardware table.

LSD15852

- First Found-in Version: CMW520-R0001P02
- Condition: Two devices connect directly. And the vlan indicated by the port's PVID not exist.
- Description: The port can't accept mstp protocol packet, and cause a fail on root bridge election.

LSD15883

- First Found-in Version: CMW520-R0001P02
- Condition: There are a lot of mac addresses in the device and display these mac by display command.
- Description: Can't stop the display of mac by enter "Ctrl+C".

LSD15888

- First Found-in Version: CMW520-R0001P02
- Condition: Firstly configure flow mirroring on a port. Secondly configure port mirroring on a port, Thirdly delete port mirror and configure port mirror on the port again
- Description: Configure port mirror on the port is failed.

LSD15927

- First Found-in Version: CMW520-R0001P02
- Condition: Insert a 100M SFP module in a GE SFP PORT.
- Description: There are some errors in the display information.

LSD16134

- First Found-in Version: CMW520-R0001P02
- Condition: Enable DHCP-SNOOPING in the device and Enable dot1x on a port. PC connects the device by the port.
- Description: PC can get IP address although PC not pass dot1x authentication.

LSD18121

- First Found-in Version: CMW520-R0001P02
- Condition: A COMBO port configured for tunnel aggregation group and save the configuration.
- Description: reboot the device and the configuration on the port is invalid.

LSD18489

- First Found-in Version: CMW520-R0001P02
- Condition: Having an Internal loopback test on a link-up 100M port.
- Description: Internal loopback test on the port is failed.

LSD19076

- First Found-in Version: CMW520-R0001P02
- Condition: SFP COMBO ports configured for tunnel aggregation group.
- Description: Remove these combo ports from aggregation group and the port status is down.

LSD19593

- First Found-in Version: CMW520-R0001P02
- Condition: Enable loopback detection in a port and there is a loopback on the port.
- Description: Static mac addresses configured on the port were deleted.

Resolved Problems in CMW520-R0001P02

LSD10803

- First Found-in Version: CMW520-E0001
- Condition: The MAC is exist, and looking up a existence MAC by specifying the condition VLAN+MAC.
- Description: Failed When Looking up the MAC.

LSD12067

- First Found-in Version: CMW520-R0001
- Condition: Firstly configuring loopback group and adding a 1000M optical port into the Loopback group. Then inserting a 1000M SFP module or 1000BAST-T module.
- Description: The Loopback configured in the Port is ineffective.

LSD14473

- First Found-in Version: CMW520-R0001
- Condition: configuring CBS value in an aggregate CAR.
- Description: The configuration operation is ineffective for the first time. Should configure twice.

LSD14489

- First Found-in Version: CMW520-R0001
- Condition: Configuring MAC address learning number is equal to 1 in a port. Then “shutdown” and “undo shutdown” in the port.
- Description: The port doesn’t learn mac address anymore.

LSD14759

- First Found-in Version: CMW520-R0001

- Condition: Configuring PVID in a port and the PVID does not exist.
- Description: The state of loopback test is error.

LSD14877

- First Found-in Version: CMW520-R0001
- Condition: The device reboot without configuration file and then undo shutdown the active combo port (the port link is up).
- Description: Appearing at several times of up/down switch.

Resolved Problems in CMW520-R0001

LSD08297

- First Found-in Version: CMW520-E0001
- Condition: Plugs 1000M SFP module into a 100M SFP slot in S3610
- Description: Link is up after loopback is enabled.

LSD08297

- First Found-in Version: CMW520-E0001
- Condition: Create a tunnel manually, do 'ping' with the packet (>1500 bytes) through the tunnel.
- Description: Fail in 'ping'.

LSD08877

- First Found-in Version: CMW520-E0001
- Condition: Create a user name with 80 characters.
- Description: Only 79 characters at most can be input when login in web.

LSD08949

- First Found-in Version: CMW520-E0001
- Condition: Configure both 'QinQ enable' and flexible QinQ.
- Description: Only basic QinQ is working, the flexible QinQ doesn't work.

LSD09713

- First Found-in Version: CMW520-E0001
- Condition: Configure ftp server, after the client is logged on.
- Description: Only directory information is printed by the command 'dir' or 'ls'.

LSD10356

- First Found-in Version: CMW520-E0001
- Condition: Configure QinQ ethernet-type on a port.
- Description: After more than 2 times changes of ethernet-type, fails to change the ether-type.

LSD11079

- First Found-in Version: CMW520-E0001

- Condition: Log on the system by web and check the system information.
- Description: Internal version is displayed in web.

Resolved Problems in CMW520-E0001

First time

Related Documentation

New Feature Documentation

Table 8 New Feature Documentation

Feature	Document title
Isolate-user-VLAN	Isolate-user-VLAN Feature Manual
PPPoE Agent	PPPoE Agent Feature Manual
IPv4 ACL rule remark	Configuring a start or end remark for ACL rules

For information about other features, see **Related Documentation**.

Documentation Set

Table 9 Related manuals

Manual	Version
H3C S3610 Series Ethernet Switches Quick Start	V1.07
H3C S3610 Series Ethernet Switches Installation Manual	V1.07
H3C S3610 Series Ethernet Switches Compliance and Safety Manual	V1.03
H3C S3610[S5510] Series Ethernet Switches Operation Manual-Feature 5315	6W101
H3C S3610[S5510] Series Ethernet Switches Command Manual-Feature 5315	6W101
H3C S5510 Series Ethernet Switches Quick Start	V1.05
H3C S5510 Series Ethernet Switches Installation Manual	V1.05
H3C S5510 Series Ethernet Switches Compliance and Safety Manual	V1.02

Obtaining Documentation

To query and download the documentation for this version, go to the website of H3C with reference of the following Table.

Table 10 Online technical support

How to apply for an account	Access the homepage of H3C at http:// www.h3c.com and click on Registration at the top right. In the displayed page, provide your information and click on Submit to register.
How to get documentation	In the homepage of H3C at http:// www.h3c.com, select Technical Support & Document > Technical Documents from the navigation menu at the top. Then select a product for its documents.

Upgrading software

You can access the Boot menu or the CLI to upgrade software images (.bin system software images and .btm Boot ROM images).

Table 11 Software upgrade methods

Method	Section
Upgrading from Boot ROM menus	Software Upgrading via Console Port (Xmodem Protocol)
	Software Upgrading via Ethernet Interface (FTP/TFTP)
	Software Upgrading via Ethernet Interface (FTP/TFTP)
Upgrading from the CLI	Software Upgrading via TFTP
	Software Upgrading via FTP

When upgrading software, make sure the versions of the Boot ROM and system software images are compatible.

The procedures for upgrading Boot ROM and system software from the Boot menu are the same except that you must choose different options from the Boot menu (**1** for upgrading system software, and **6** for upgrading Boot ROM) to start the upgrade procedure. This appendix describes only the Boot ROM upgrade procedure.

Upgrading software from Boot ROM menus

To upgrade software from Boot ROM menus:

1. Connect a configuration terminal such as a PC to the console port of the switch with a console cable.
2. Run the terminal emulation program on the PC.
3. Power on the switch.

   The switch starts up and displays the following message:

```
System is starting...................

            ************************************************************
            *                                                          *
            *             H3C S3610-52P BOOTROM, Ver 213               *
            *                                                          *
            ************************************************************
```

```
Copyright (c) 2004-2013 Hangzhou H3C Technologies Co., Ltd.
Compiled Date       : Jan  9 2013
CPU Clock Speed     : 200MHz
Memory Size         : 128MB
CPLD Version        : 001
PCB Version         : Ver.B

Board checking.....................................LSA1LTSG
SDRAM fast selftest................................OK!
Flash fast selftest................................OK!
CPLD selftest......................................OK!
Switch chip selftest...............................OK!
Slot 1/1/1 has no module or get slot type error
Slot 1/1/2 has no module or get slot type error
Slot 1/1/3 has no module or get slot type error
Slot 1/1/4 has no module or get slot type error
PHY selftest.......................................OK!
Please check port leds.........................finished!

The switch Mac is: 00E0-FC00-3900


Press Ctrl-B to enter Boot Menu...
Please input BootROM password:

BootRom password: Not required. Please press Enter to continue.
```

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

   ```
   BootRom password: Not required. Please press Enter to continue.
   ```

2. Press **Enter** at the prompt for password.

   The "Password recovery capability is enabled." or "Password recovery capability is disabled." message appears, followed by the Boot menu. Availability of some menu options depends on the state of password recovery capability (see Table 2). For more information about password recovery capability, see *H3C S3610_5510-CMW520-R5319P04 Release Notes*.

   ```
   Password recovery capability is enabled.


      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. Restore to factory default configuration
   6. Enter BootRom upgrade menu
   7. Skip current system configuration
   8. Reserved
   ```

```
9. Set switch startup mode
0. Reboot

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

Table 12 Extended Boot ROM menu options

Option	Tasks
1. Download application file to flash	Download a .bin software package file to the flash. If password recovery capability is enabled, you can use any version of the system software image for upgrade. If password recovery capability is disabled, you can use only the R5319P04 version (or higher) for upgrade.
2. Select application file to boot	Specify the system software images for the next startup: • If password recovery capability is enabled, you can specify a system software image of any version. • If password recovery capability is disabled, the system software image version must be R5319P04or higher.
3. Display all files in flash	Display files on the flash.
4. Delete file from flash	Delete files to free storage space.
5. Restore to factory default configuration	Delete the current next-startup configuration files and restore the factory-default configuration. This option is available only if password recovery capability is disabled.
6. Enter BootRom upgrade menu	Access the Boot ROM upgrade menu. If password recovery capability is enabled, you can upgrade the Boot ROM to any version. If password recovery capability is disabled, you can upgrade the Boot ROM to only Version 213 or higher.
7. Skip current system configuration	Start the switch without loading any configuration file. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. This option is available only if password recovery capability is enabled.
8. Reserved	Reserved option field.
9. Set switch startup mode	Set the startup mode to fast startup mode or full startup mode.
0. Reboot	Reboot the switch.

Software Upgrading via Console Port (Xmodem Protocol)

Step 1: Enter **1** in the Boot menu. Press <Enter> and the system will 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 to boot menu
Enter your choice(0-3):3
```

Step 2: Enter **3** in the download program menu. Select to implement the software upgrading via Xmodem protocol. Press <Enter> and the screen will display the following information:

```
Please select your download baudrate:
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. Return
Enter your choice (0-5):
```

Step 3: Select the appropriate download speed based on the actual requirements. For example, enter **5** to select the download speed as 115200bps. Press <Enter> and the system will display the following information:

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

Step 4: Follow the above prompt and change the baud rate on the console terminal, so that the baud rate is consistent with the selected download baud rate of the software. After the baud rate setting at the console terminal is completed, disconnect the terminal and reconnect it. Press <Enter> to start downloading, and the screen will display the following information:

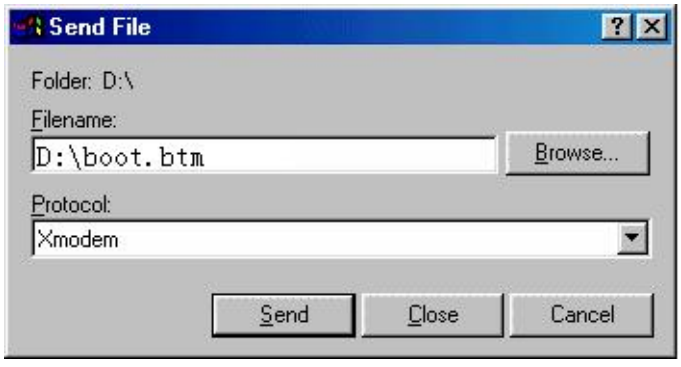
```
Are you sure to download file to flash? Yes or No(Y/N)y
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Downloading ... CCCCC
```

NOTE:

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.

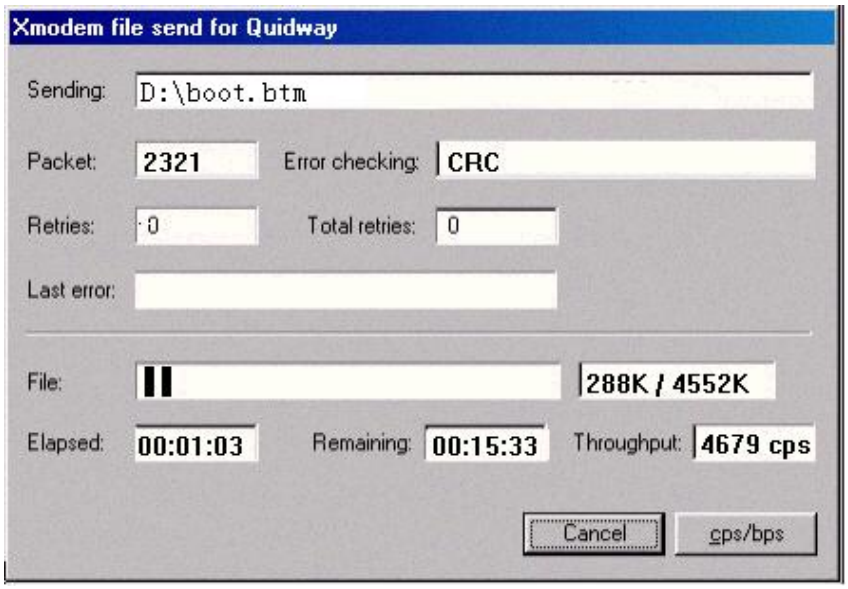
Step 5: Select [Transfer\Send File] from the terminal window. Click <Browse> in the pop-up window (as shown Figure 1) and select the software to be downloaded. Change the protocol name to Xmodem.

Figure 1 Send File



Step 6: Click <Send> and the system will display the window as shown Figure 2 .

Figure 2 Xmodem File Send



Step 7: After the downloading of the program is completed, the screen will display the following information:

```
Loading ..............................................................done
Writing to flash......................................................done
```

Software Upgrading via Ethernet Interface (FTP/TFTP)

Software Upgrading via TFTP

1. Introduction to TFTP

TFTP (trivial file transfer protocol) is a type of simple file transfer protocol in the TCP/IP protocol suite that applies between clients and servers. TFTP is normally realized on the UDP basis to provide unreliable data transfer service.

2. TFTP upgrading procedure

Step 1: Select an Ethernet interface for downloading on the S3610. Connect the switch to the PC (where the upgrading file is located) via the interface. At the same time, you should connect the switch to a PC via the console port (The PC should be the same as the PC where the upgrading file is located).

Step 2: Run the TFTP server program on the PC connected with the Ethernet interface for upgrading, and specify the file path of the upgrading program.

△ **CAUTION:**

H3C series switches are not shipped with TFTP Server program.

Step 3: Run the terminal emulation program on the PC connected to the Console port, and boot the switch to access the Boot menu.

Step 4: Enter **1** in the Boot menu. Press <Enter> and the system will 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 to boot menu
Enter your choice(0-3):1
```

Step 5: Enter **1** in the download program menu. Select to use TFTP for the software upgrading. Press <Enter> and the screen will display the following information:

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

Step 6: Complete the relevant information based on the actual requirements and press <Enter>. The screen will display the following information:

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

Step 7: Enter **Y** and the system starts downloading the file. Enter **N** and the system will return to Boot menu. Take entering **Y** as an example. Enter **Y** and press <Enter>, the system begins downloading programs. After the downloading is completed, the system starts write-flash operation. Upon completion of this operation, the screen displays the following information to indicate that the downloading is completed:

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

Software Upgrading via FTP

1. Introduction to FTP

Through the Ethernet port, the S3610 can serve as an FTP server or client. It provides another means to download the system program and configure the files. In the following description we assume that the S3610 serves as an FTP client.

2. FTP upgrading procedure

Step 1: Select an Ethernet interface for downloading on the S3610. Connect the switch to the PC (where the upgrading file is located and whose IP address should be known) via the interface. At the same time, you should connect the switch to a PC via the Console port (the PC should be the same as the PC where the upgrading file is located).

Step 2: Run the FTP server program on the PC connected to the Ethernet interface for upgrading, and specify the file path of the upgrading program.

Step 3: Run the terminal emulation program on the PC connected to the Console port, and boot the switch to access the Boot menu.

Step 4: Enter **1** in the Boot menu. Press <Enter> and the system will 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 to boot menu
Enter your choice(0-3):2
```

Step 5: Enter **2** in the download program menu. Select FTP for the software upgrading. Press <Enter> and the screen will display the following information:

```
Please modify your FTP protocol parameter:
Load File name
Switch IP address
Server IP address
FTP User Name
FTP User Password
```

Step 6: Complete the relevant information based on the actual requirements and press <Enter>. The screen will display the following information:

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

Step 7: Enter **Y** and the system starts downloading the file. Enter **N** and the system will return to Boot menu. Take the first case as an example. Enter **Y** and press <Enter>, the system begins downloading programs. After the downloading is completed, the system starts write-flash operation. Upon completion of this operation, the screen displays the following information to indicate that the downloading is completed:

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

Appendix

Details of Added CLI Commands in CMW520-F5315

ip check source ipv6

Syntax

ip check source ipv6 { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip check source ipv6

View

Ethernet interface view, VLAN interface view

Default Level

2: System level

Parameters

ipv6: Specifies IPv6 source guard dynamic binding. Without this keyword, this command displays IPv4 source guard dynamic binding entries. Support for this keyword depends on the device model.

ip-address: Specifies to bind source IP addresses to the port. Support for this keyword depends on the device model.

ip-address mac-address: Specifies to bind source IP addresses and MAC addresses to the port. Support for this keyword depends on the device model.

mac-address: Specifies to bind source MAC addresses to the port. Support for this keyword depends on the device model.

Description

Use the **ip check source** command to configure the IP soruce guard dynamic binding function on a port.

Use the **undo ip check source** command to restore the default.

By default, the IP source guard dynamic binding function is disabled.

Note that:

You cannot configure the IP source guard dynamic binding function on a port that is in an aggregation group or a service loopback group.

Support for the IPv4 source guard dynamic binding function on a Layer 3 Ethernet port depends on the device model.

IPv6 source guard dynamic binding can be configured only in Layer 2 Ethernet port view.

user-bind ipv6

Syntax

user-bind ipv6 { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo user-bind ipv6 { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

ipv6: Specifies to bind an IPv6 address. Without this keyword, an IPv4 address is bound. Support for this keyword depends on the device model.

ip-address ip-address: Specifies the IP address for the static binding. The IPv4 address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0. The IPv6 address cannot be all 0s, a multicast address, or a loopback address. Support for the ip-address argument depends on the device model.

mac-address mac-address: Specifies the MAC address for the static binding in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address. Support for the mac-address argument depends on the device model.

vlan vlan-id: Specifies the VLAN for the static binding. vlan-id is the ID of the VLAN to be bound, in the range 1 to 4094. Support for vlan vlan-id depends on the device model.

Description

Use the **user-bind** command to configure a static binding.

Use the **undo user-bind** command to delete a static binding.

By default, no static binding exists on a port.

Note that:

The maximum number of binding entries that can be configured varies by device.

You cannot configure a static binding on a port that is in an aggregation group or a service loopback group

ipv6 dhcp snooping enable

Syntax

ipv6 dhcp snooping enable

undo ipv6 dhcp snooping enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 dhcp snooping enable** command to enable DHCPv6 snooping globally.

Use the **undo ipv6 dhcp snooping enable** command to disable global DHCPv6 snooping.

By default, global DHCPv6 snooping is disabled.

After DHCPv6 snooping is enabled in system view, the DHCPv6 snooping device discards DHCPv6 reply messages received by an untrusted port if any, and does not record DHCPv6 entries.

ipv6 dhcp snooping vlan enable

Syntax

ipv6 dhcp snooping vlan enable

undo ipv6 dhcp snooping vlan enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 dhcp snooping vlan enable** command to enable DHCPv6 snooping for a specific VLAN.

Use the **undo ipv6 dhcp snooping vlan enable** command to disable DHCPv6 snooping for a specific VLAN.

By default, DHCPv6 snooping is disabled for a VLAN.

After DHCPv6 snooping is enabled in VLAN view, the DHCPv6 snooping device records DHCPv6 snooping entries according to the DHCPv6 packets received in the VLAN. Meanwhile, upon receiving a DHCPv6 request from a client in the VLAN, the device forwards the packet through a trusted port rather than any untrusted port in the VLAN, thus reducing network traffic.

ipv6 nd snooping enable

Syntax

ipv6 nd snooping enable

undo ipv6 nd snooping enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping enable** command to enable ND snooping.

Use the **undo ipv6 nd snooping enable** command to restore the default.

By default, ND snooping is disabled.

ipv6 nd detection enable

Syntax

ipv6 nd detection enable

undo ipv6 nd detection enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 nd detection enable** command to enable ND detection in a VLAN to check ND packets for source spoofing.

Use the **undo ipv6 nd detection enable** command to disable ND detection.

By default, ND detection is disabled.

pim ipv6

Syntax

pim ipv6

undo pim ipv6

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6** command to enter IPv6 PIM view.

Use the **undo pim ipv6** command to remove all configurations performed in IPv6 PIM view.

Note that IPv6 multicast routing must be enabled on the device before this command can take effect.

pim ipv6 dm

Syntax

pim ipv6 dm

undo pim ipv6 dm

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 dm** command to enable IPv6 PIM-DM.

Use the **undo pim ipv6 dm** command to disable IPv6 PIM-DM.

By default, IPv6 PIM-DM is disabled.

Note that:

This command can take effect only after IPv6 multicast routing is enabled on the device.

IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

pim ipv6 sm

Syntax

pim ipv6 sm

undo pim ipv6 sm

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **pim ipv6 sm** command to enable IPv6 PIM-SM.

Use the **undo pim ipv6** sm command to disable IPv6 PIM-SM.

By default, IPv6 PIM-SM is disabled.

Note that this command can take effect only after IPv6 multicast routing is enabled on the device.

ssm-policy

Syntax

ssm-policy *acl6-number*

undo ssm-policy

View

IPv6 PIM view

Default Level

2: System level

Parameters

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999.

Description

Use the **ssm-policy** command to configure the IPv6 SSM group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the IPv6 SSM group range is FF3x::/32. Here x refers to any legal scope.

This command allows you to define an address range of permitted or denied IPv6 multicast groups. If the match succeeds, the running multicast mode will be IPv6 PIM-SSM; otherwise the multicast mode will be IPv6 PIM-SM.

group-policy

Syntax

group-policy *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

IGMP-Snooping view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX or TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan vlan-list: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of vlan-id, or a VLAN range in the form of start-vlan-id to end-vlan-id, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **group-policy** command to configure a global multicast group filter, namely to control the multicast groups a host can join.

Use the **undo group-policy** command to remove the configured global multicast group filter.

By default, no global multicast group filter is configured, namely a host can join any valid multicast group.

Note that:

If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.

You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

igmp-snooping group-policy

Syntax

igmp-snooping group-policy *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

View

Ethernet interface view, Layer 2 aggregate interface view, port group view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan vlan-list: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of vlan-id, or a VLAN range in the form of start-vlan-id to end-vlan-id, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **igmp-snooping group-policy** command to configure a multicast group filter on the current port(s), namely to control the multicast groups hosts on the port(s) can join.

Use the **undo igmp-snooping group-policy** command to remove a multicast group filter on the current port(s).

By default, no multicast group filter is configured on an interface, namely a host can join any valid multicast group.
Note that:

If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you

specify a VLAN or multiple VLANs, the command will take effect only if the interface belongs to the specified VLAN(s).

If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.

You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

mld-snooping group-policy

Syntax

mld-snooping group-policy *acl6-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

View

Ethernet interface view, Layer 2 aggregate interface view, port group view

Default Level

2: System level

Parameters

acl6-number: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The IPv6 source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan vlan-list: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of vlan-id, or a VLAN range in the form of start-vlan-id to end-vlan-id, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **mld-snooping group-policy** command to configure an IPv6 multicast group filter on the current port(s), namely to control the multicast groups hosts on the port(s) can join.

Use the **undo mld-snooping group-policy** command to remove the configured IPv6 multicast group filter on the current port(s).

By default, no IPv6 multicast group filter is configured on a port, namely a host can join any valid IPv6 multicast group.
Note that:

If you do not specify any VLAN when using this command in Ethernet interface view or Layer 2 aggregate interface view, the command will take effect for all VLANs the interface belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the interface belongs to the specified VLAN(s).

If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

group-policy

Syntax

group-policy *acl6-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

MLD-Snooping view

Default Level

2: System level

Parameters

Acl6-number: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule is used to match the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan vlan-list: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of vlan-id, or a VLAN range in the form of start-vlan-id to end-vlan-id, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **group-policy** command to configure a global IPv6 multicast group filter, namely to control the IPv6 multicast groups a host can join.

Use the **undo group-policy** command to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally, namely any host can join any valid IPv6 multicast group.

Note that:

If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.

You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

cfd version

Syntax

cfd version { **draft5** | **draft5-plus** | **standard** }

undo cfd version

View

System view

Default Level

2: System level

Parameters

draft5: Specifies that IEEE 802.1ag draft5.2 be used.

draft5-plus: Specifies that the IEEE 802.1ag draft5.2 interim version be used.

standard: Specifies that the standard version of IEEE 802.1ag be used.

Description

Use the **cfd version** command to configure the CFD protocol version.

Use the **undo cfd version** command to restore the default.

By default, CFD uses the standard version of IEEE 802.1ag.

cfd slm service-instance

Syntax

cfd slm service-instance *instance-id* **mep** *mep-id* { t**arget-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

System view

Default Level

2: System level

Parameters

service-instance instance-id: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep mep-id: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac mac-address: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep target-mep-id: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number number: Specifies the number of LMM frames sent. The number argument ranges from 2 to 10, and defaults to 5.

Description

Use the **cfd slm** command to enable LM. The LM function measures the frame loss between two MEPs by sending LMM frames out of the source MEP to the target MEP and detecting the returned LMRs.

By default, LM is disabled.

The LM function takes effect in only CFD IEEE 802.1ag.

cfd dm one-way service-instance

Syntax

cfd dm one-way service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

System view

Default Level

2: System level

Parameters

service-instance instance-id: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep mep-id: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac mac-address: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep target-mep-id: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number number: Specifies the number of 1DM frames sent. The number argument ranges from 2 to 10, and defaults to 5.

Description

Use the **cfd dm one-way** command to enable one-way DM. The one-way DM function measures the one-way frame delay between two MEPs by sending 1DM frames out of a MEP to the target MEP.

By default, one-way DM is disabled.

Note that:

The one-way DM function takes effect in only CFD IEEE 802.1ag.

To view the one-way delay test result, use the display cfd dm one-way history command on the target MEP.

cfd dm two-way service-instance

Syntax

cfd dm two-way service-instance *instance-id* **mep** *mep-id* { **target-mac** *mac-address* | **target-mep** *target-mep-id* } [**number** *number*]

View

System view

Default Level

2: System level

Parameters

service-instance instance-id: Specifies a service instance by its ID, which ranges from 1 to 32767.

mep mep-id: Specifies the source MEP by its ID, which ranges from 1 to 8191.

target-mac mac-address: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep target-mep-id: Specifies the target MEP by its ID, which ranges from 1 to 8191.

number number: Specifies the number of DMM frames sent. The number argument ranges from 2 to 10, and defaults to 5.

Description

Use the **cfd dm two-way** command to enable two-way DM. The two-way DM function measures the two-way frame delay between two MEPs by sending DMM frames to the target MEP and detecting the responded DMR frames.

By default, two-way DM is disabled.

The two-way DM function takes effect in only CFD IEEE 802.1ag.

multicast ipv6 routing-enable

Syntax

multicast ipv6 routing-enable

undo multicast ipv6 routing-enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **multicast ipv6 routing-enable** command to enable IPv6 multicast routing.

Use the **undo multicast ipv6 routing-enable** command to disable IPv6 multicast routing.

IPv6 multicast routing is disabled by default.

Note that:

You must enable IPv6 multicast routing before you can carry out other Layer 3 IPv6 multicast commands.

The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

ipv6 mtu

Syntax

ipv6 mtu *mtu-size*

undo ipv6 mtu

View

Interface view

Default Level

2: System level

Parameters

mtu-size: Size of the maximum transmission units (MTUs) of an interface in bytes. The value range depends on the device model.

Description

Use the **ipv6 mtu** command to set the MTU of IPv6 packets sent over an interface.

Use the **undo ipv6 mtu** command to restore the default MTU.

multicast-vlan ipv6

Syntax

multicast-vlan ipv6 *vlan-id*

undo multicast-vlan ipv6 { **all** | *vlan-id* }

View

System view

Default Level

2: System level

Parameters

vlan-id: Specifies a VLAN by its ID, in the range of 1 to 4094.

all: Deletes all IPv6 multicast VLANs.

Description

Use the **multicast-vlan ipv6** command to configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use the **undo multicast-vlan ipv6** command to remove the specified VLAN as an IPv6 multicast VLAN.

No VLAN is an IPv6 multicast VLAN by default.

Note that:

The specified VLAN to be configured as an IPv6 multicast VLAN must exist.

The IPv6 multicast VLAN feature cannot be enabled on a device with IPv6 multicast routing enabled.

For a sub-VLAN-based IPv6 multicast VLAN, you need to enable MLD Snooping only in the IPv6 multicast VLAN; for a port-based IPv6 multicast VLAN, you need to enable MLD Snooping in both the IPv6 multicast VLAN and all the user VLANs.

subvlan

Syntax

subvlan vlan-list

undo subvlan { **all** | *vlan-list* }

View

IPv6 multicast VLAN view

Default Level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of vlan-id, or a VLAN range in the form of start-vlan-id to end-vlan-id, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

all: Deletes all the sub-VLANs of the current IPv6 multicast VLAN.

Description

Use the **subvlan** command to configure sub-VLAN(s) for the current IPv6 multicast VLAN.

Use the **undo subvlan** command to remove the specified sub-VLAN(s) or all sub-VLANs from the current IPv6 multicast VLAN.

An IPv6 multicast VLAN has no sub-VLANs by default.

Note that:

- The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of another IPv6 multicast VLAN.
- The number of sub-VLANs of the IPv6 multicast VLAN must not exceed the system-defined limit (this limit varies with different device models).

ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

View

Interface view

Default Level

2: System level

Parameters

number: Maximum number of neighbors that can be dynamically learned by the interface.

Description

Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on the interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

isolated-vlan enable

Syntax

isolated-vlan enable

undo isolated-vlan enable

View

VLAN view

Default Level

2: System level

Parameters

None.

Description

Use the isolated-vlan enable command to enable the sub-VLAN, which in a super-VLAN, isolated-vlan mode.

Use the undo isolated-vlan enable command to disable the sub-VLAN, which in a super-VLAN, isolated-vlan mode.

By default, isolated-vlan mode is not enabled.

authorization command

Syntax

authorization command { **hwtacacs-scheme hwtacacs-scheme-name** [**local** | **none**] | **local** | **none** }

undo authorization command

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme hwtacacs-scheme-name: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the corresponding default rights.

Description

Use the **authorization command** command to configure the command line authorization method.

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

By default, the default authorization method is used for command line users.

Note that:

- The HWTACACS scheme specified for the current ISP domain must have been configured.
- For local authorization, the local users must have been configured for the command line users on the device, and the level of the commands authorized to a local user must be lower than or equal to that of the local user. Otherwise, local authorization will fail.

oam timer hello

Syntax

oam timer hello *interval*

undo oam timer hello

View

System view

Default Level

2: System level

Parameters

interval: Ethernet OAM handshake packet transmission interval, in milliseconds. The value of this argument must be a multiple of 100, while the value range of this argument depends on your device model.

Description

Use the **oam timer hello** command to configure the Ethernet OAM handshake packet transmission interval.

Use the **undo oam timer hello** command to restore the default.

By default, the Ethernet OAM handshake packet transmission interval is 1000 milliseconds.

Note that:

after the timeout timer for an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to be disconnected. Therefore, you are recommended to set the connection timeout timer at least five times the handshake packet transmission interval, thus ensuring the stability of Ethernet OAM connections.

oam timer keepalive

Syntax

oam timer keepalive *interval*

undo oam timer keepalive

View

System view

Default Level

2: System level

Parameters

interval: Ethernet OAM connection timeout timer, in milliseconds. The value of this argument must be a multiple of 100, while the value range of this argument depends on your device model.

Description

Use the **oam timer keepalive** command to configure the Ethernet OAM connection timeout timer.

Use the **undo oam timer keepalive** command to restore the default.

By default, the Ethernet OAM connection timeout timer is 5000 milliseconds.

Note that:

after the timeout timer for an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to be disconnected. Therefore, you are recommended to set the connection timeout timer at least five times the handshake packet transmission interval, thus ensuring the stability of Ethernet OAM connections.

user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

View

System view

Default Level

2: System level

Parameters

profile-name: Use profile name, a string of 1 to 31 characters, case sensitive. It can only contain English letters, numbers, underlines, and must start with an English letter. A user profile name must be globally unique.

Description

Use the **user-profile** command to create a user profile and enter the corresponding user profile view. If the specified user profile already exists, you will directly enter the corresponding user profile view, without the need to create a user profile.

Use the **undo user-profile** command to remove an existing, disabled user profile.

By default, no user profiles exist on the device.

An enabled user profile cannot be removed.

user-profile enable

Syntax

user-profile *profile-name* **enable**

undo user-profile *profile-name* **enable**

View

System view

Default Level

2: System level

Parameters

profile-name: Use profile name, a string of 1 to 31 characters, case sensitive. It can only contain English letters, numbers, underlines, and must start with an English letter.

Description

Use the **user-profile enable** command to enable a user profile.

Use the **undo user-profile enable** command to disable the specified user profile.

By default, a created user profile is disabled.

Note that:

When you execute the command, the specified user profile must be created; otherwise, the command fails.

Only an enabled user profile can be used by users. You cannot modify or remove the configuration items in a user profile until the user profile is disabled.

Disabling a user profile logs out the users using the user profile.

qos apply policy

Syntax

qos apply policy *policy-name* **inbound**

undo qos apply policy inbound

View

User profile view

Default Level

2: System level

Parameters

inbound: Applies the QoS policy to the incoming traffic of online users.

policy-name: Policy name, a string of 1 to 31 characters.

Description

Use the **qos apply policy** command to apply a QoS policy to a user profile.

Use the **undo qos apply policy** command to remove the QoS policy.

Note that:

- If a user profile is activated, the QoS policy, except the ACLs referenced in the QoS policy, applied to it cannot be configured or removed. When the users of the user profile are online, the referenced ACLs cannot be modified either.
- The QoS policy applied to a user profile takes effect when the user-profile is activated and the corresponding users are online.
- Only the remark, car, and filter actions are supported in the QoS policies applied in user profile view.
- A null policy cannot be applied in user profile view.

Details of Added CLI Commands in CMW520-F5316

display isolate-user-vlan

Syntax

display isolate-user-vlan [*isolate-user-vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

isolate-user-vlan-id: Isolate-user-VLAN ID, in the range of 1 to 4094.

|: 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 isolate-user-vlan** command to display the mapping between an isolate-user-VLAN and secondary VLANs and information about these VLANs.

Related commands: **isolate-user-vlan** and **isolate-user-vlan enable**.

Examples

Display the mapping between an isolate-user-VLAN and secondary VLANs and information about these VLANs.

```
<Sysname> display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 2
 Secondary VLAN ID : 3 4

 VLAN ID: 2
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: configured
 IP Address: 1.1.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   Ports: none
```

```
Untagged Ports:
   Ethernet1/0/2            Ethernet1/0/3            Ethernet1/0/4

VLAN ID: 3
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: configured
IP Address: 2.2.2.2
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: none
Untagged Ports:
   Ethernet1/0/2            Ethernet1/0/3

VLAN ID: 4
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged   Ports: none
Untagged Ports:
Ethernet1/0/2            Ethernet1/0/4
```

isolate-user-vlan

Syntax

isolate-user-vlan *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]

undo isolate-user-vlan *isolate-user-vlan-id* [**secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]]

View

System view

Default Level

2: System level

Parameters

isolate-user-vlan-id: Isolate-user-VLAN ID, in the range 1 to 4094.

secondary *secondary-vlan-id* [**to** *secondary-vlan-id*]: Specifies a secondary VLAN ID or a secondary VLAN ID range. The *secondary-vlan-id* argument is a secondary VLAN ID, in the range 1 to 4094.

Description

Use the **isolate-user-vlan** command to associate an isolate-user-VLAN with the specified secondary VLANs.

Use the **undo isolate-user-vlan** command to remove the association.

By default, an isolate-user-VLAN is not associated with any secondary VLAN.

- The **undo isolate-user-vlan** command without the **secondary** *secondary-vlan-id* parameter specified removes the association between the specified isolate-user-VLAN and all its secondary VLANs, while the **undo isolate-user-vlan** command with the **secondary** *secondary-vlan-id* parameter specified only removes the association between the specified isolate-user-VLAN and the specified secondary VLANs.
- After associating an isolate-user-VLAN with the specified secondary VLANs, you cannot add/remove an access port to/from an involved VLAN or delete an involved VLAN. To do that, cancel the association first.

Related commands: **display isolate-user-vlan**.

Examples

Associate isolate-user-VLAN 2 with secondary VLANs VLAN 3 and VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] port ethernet 1/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port ethernet 1/0/3
[Sysname-vlan3] vlan 4
[Sysname-vlan4] port ethernet 1/0/4
[Sysname-vlan4] quit
[Sysname] isolate-user-vlan 2 secondary 3 to 4
```

isolate-user-vlan enable

Syntax

isolate-user-vlan enable

undo isolate-user-vlan enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **isolate-user-vlan enable** command to configure the current VLAN as an isolate-user-VLAN.

Use the **undo isolate-user-vlan enable** command to remove the isolate-user-VLAN configuration for the current VLAN.

By default, no VLAN is an isolate-user-VLAN.

An isolate-user-VLAN may include multiple ports, including the one connected to the upstream device.

Related commands: **display isolate-user-vlan**.

Examples

Configure VLAN 5 as an isolate-user-VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] isolate-user-vlan enable
```

isolated-vlan enable

Syntax

isolated-vlan enable

undo isolated-vlan enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **isolated-vlan enable** command to isolate ports in the same secondary VLAN at Layer 2.

Use the **undo isolated-vlan enable** command to restore the default.

By default, ports in the same secondary VLAN are not isolated at Layer 2.

- This command is not applicable to an isolate-user-VLAN.
- Layer 2 isolation configured with the **isolated-vlan enable** command takes effect only after the secondary VLAN is associated with an isolate-user-VLAN and configured the isolate-user-VLAN type of a port.
- To configure this command for a secondary VLAN, make sure that the secondary VLAN is not associated with an isolate-user-VLAN.

Examples

Isolate ports in secondary VLAN 4 at Layer 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] port ethernet 1/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port ethernet 1/0/3
[Sysname-vlan3] vlan 4
[Sysname-vlan4] port ethernet 1/0/4
[Sysname-vlan4] quit
[Sysname] isolate-user-vlan 2 secondary 3 to 4
[Sysname] vlan 4
[Sysname-vlan4] isolated-vlan enable
```

port isolate-user-vlan

Syntax

port isolate-user-vlan { **host** | **promiscuous** }

undo port isolate-user-vlan

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

host: Configures the port as a downstream port.

promiscuous: Configures the port as an upstream port.

Description

Use the **port isolate-user-vlan** command to configure the isolate-user-VLAN type of a port.

Use the **undo port isolate-user-vlan** command to restore the default setting.

By default, no isolate-user-VLAN type is configured for a port.

Related commands: **isolate-user-vlan**.

Examples

Configure the access port Ethernet 1/0/1 as a downstream port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] port isolate-user-vlan host
```

Configure the Layer 2 aggregate interface Bridge-Aggregation 1 as a hybrid port and then configure it as an upstream port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port isolate-user-vlan promiscuous
```

port bridge enable

Syntax

port bridge enable

undo port bridge enable

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **port bridge enable** command to enable bridging on a Layer 2 Ethernet interface.

Use the **undo port bridge enable** command to disable bridging on the Ethernet interface.

By default, bridging is not enabled on Layer 2 Ethernet interfaces.

Normally, if the outgoing interface in the MAC address entry for a packet is the same as the incoming interface where the packet arrived, the packet is dropped. The bridging function enables an Ethernet port to forward such packets.

Details of Added CLI Commands in CMW520-F5317

display pppoe agent information format

Syntax

display pppoe agent information format [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

|: 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 all 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 pppoe agent information format** command to display the format and content of fields attached to the PPPoE packet.

Examples

Display the format and content of fields added to the PPPoE packet

```
<Sysname> display pppoe agent information format
The current information format:
  Circuit ID: common
  Remote ID: extend
```

Table 13 display pppoe agent information format command output description

Field	Description
Circuit ID	Format of the circuit-id, which can be: • common—Standard format. • extend—Extended format. • Character string—User-defined format.
Remote ID	Format of the remote-id, which can be: • common—Standard format. • extend—Extend format. • Character string—User-defined format.

display pppoe agent information policy

Syntax

display pppoe agent information policy [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

|: 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 all 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 pppoe agent information policy** command to display the handling policy for the original circuit-id and remote-id fields in the PPPoE packet.

Examples

Display the handing policy for the original circuit-id and remote-id fields in the PPPoE packet.

```
<Sysname> display pppoe agent information policy
The global current information policy: drop
The port Ethernet1/0/1 current information policy: replace
```

Table 14 display pppoe agent information policy command output description

Field	Description

Field	Description
The global current information policy	The global handing policy for the original circuit-id and remote-id fields in a PPPoE packet, which can be: • **drop**—Drops the original circuit-id and remote-id fields of a PPPoE packet. • **replace**—Replaces the original circuit-id and remote-id fields of a PPPoE packet with the circuit-id and remote-id fields on the switch. • **keep**—Keeps the original circuit-id and remote-id fields of a PPPoE packet.
The port Ethernet1/0/1 current information policy	The handing policy for the original circuit-id and remote-id fields in a PPPoE packet on a port, which can be: • **drop**—Drops the original circuit-id and remote-id fields of a PPPoE packet. • **replace**—Replaces the original circuit-id and remote-id fields of the PPPoE packet with the circuit-id and remote-id fields on the switch. • **keep**—Keeps the original circuit-id and remote-id fields of a PPPoE packet.

pppoe agent information enable

Syntax

pppoe agent information enable

undo pppoe agent information enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **pppoe agent information enable** command to enable the PPPoE agent function on the switch. A PPPoE-agent-enabled switch attaches the access information of PPPoE clients to the PPPoE packets from the PPPoE clients to the PPPoE server.

Use the **undo pppoe agent information enable** command to disable the PPPoE agent function.

By default, the PPPoE agent function is disabled.

Examples

Enable the PPPoE agent function on the switch.

```
<Sysname> system-view
[Sysname] pppoe agent information enable
```

pppoe agent information format circuit-id

Syntax

pppoe agent information format circuit-id { **common** | **extend** | **user-defined** *text* }

undo pppoe agent information format circuit-id

View

System view

Default Level

2: System level

Parameters

common: Standard format.

extend: Extended format.

user-defined: User-defined format.

text: Content in user-defined format, a string of 1 to 127 characters.

Description

Use the **pppoe agent information format circuit-id** command to configure the format and content for the circuit ID field attached to the PPPoE packet.

Use the **undo pppoe agent information format circuit-id** command to restore the default.

By default, the circuit ID format is **common**.

Examples

Configure the circuit ID format as **extend**.

```
<Sysname> system-view
[Sysname] pppoe agent information format circuit-id extend
```

pppoe agent information format remote-id

Syntax

pppoe agent information format remote-id { **common** | **extend** | **user-defined** *text* }

undo pppoe agent information format remote-id

View

System view

Default Level

2: System level

Parameters

common: Standard format.

extend: Extended format.

user-defined: User-defined format.

text: Content in user-defined format, a string of 1 to 127 characters.

Description

Use the **pppoe agent information format remote-id** command to configure the format and content for the remote ID field attached to the PPPoE packet.

Use the **undo pppoe agent information format remote-id** command to restore the default.

By default, the remote ID format is **common**.

Examples

Configure the remote ID format as **extend**.

```
<Sysname> system-view
[Sysname] pppoe agent information format remote-id extend
```

pppoe agent information node-identifier

Syntax

pppoe agent information node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }

undo pppoe agent information node-identifier

View

System view

Default Level

2: System level

Parameters

mac: Uses the node's MAC address as the node identifier.

sysname: Uses the device name of a node as the node identifier.

user-defined *node-identifier*: Uses a specified character string as the node identifier. *node-identifier* is a string of 1 to 50 characters.

Description

Use the **pppoe agent information node-identifier** command to configure the format and content for the node ID field attached to the PPPoE packet.

Use the **undo pppoe agent information node-identifier** command to restore the default.

By default, the node ID format is **mac**.

Examples

Configure the node ID format as **sysname**.

```
<Sysname> system-view
[Sysname] pppoe agent information node-identifier sysname
```

pppoe agent information policy

Syntax

pppoe agent information policy { **drop** | **replace** | **keep** }

undo pppoe agent information policy

View

System view, Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

drop: Drops the original circuit-id and remote-id fields of a PPPoE packet.

replace: Replaces the original circuit-id and remote-id fields of a PPPoE packet.

keep: Keeps the original circuit-id and remote-id fields of a PPPoE packet.

Description

Use the **pppoe agent information policy** command to configure the handing policy for the original circuit-id and remote-id fields in the PPPoE packet.

Use the **undo pppoe agent information policy** command to restore the default.

By default, the global handing policy is replacing the original circuit-id and remote-id fields in the PPPoE packet, and no handing policy is configured on a port.

A port preferably uses the handling policy configured on the port (if there is any) over the global handing policy.

Examples

Configure the PPPoE agent to globally drop the original circuit-id and remote-id fields in the PPPoE packet.

```
<Sysname> system-view
[Sysname] pppoe agent information policy drop
```

Configure port Ethernet 1/0/1 to replace the original circuit-id and remote-id fields in the PPPoE packet.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] pppoe agent information policy replace
```

pppoe agent uplink-port trust

Syntax

pppoe agent uplink-port trust

undo pppoe agent uplink-port trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **pppoe agent uplink-port trust** command to configure a port as trusted.

Use the **undo pppoe agent uplink-port trust** command to restore the default.

By default, all ports are untrusted.

NOTE:

To ensure normal operation of the PPPoE agent, configure the port connecting to the PPPoE server on the PPPoE-agent-enabled switch as trusted.

The trusted port configuration takes effect only on the PPPoE packets at the discovery phase.

An S3610 series Ethernet switch supports up to ten trusted ports.

Examples

Configure port Ethernet 1/0/1 as a trusted port.

```
< Sysname> system-view
[Sysname] interface ethernet 1/0/1
[Sysname-Ethernet1/0/1] pppoe agent uplink-port trust
```

traffic-pppoe

Syntax

traffic-pppoe source-address { *mac-address* | **any** } **destination-address** { *mac-address* | **any** }

undo traffic-pppoe source-address { *mac-address* | **any** } **destination-address** { *mac-address* | **any** }

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

mac-address: MAC address to be matched.

any: Any MAC address.

Description

Use the **traffic-pppoe source-address** command to configure a flow control rule for PPPoE packets.

Use the **undo traffic-pppoe source-address** command to delete a flow control rule for PPPoE packets.

By default, no flow control rule is configured for PPPoE packets.

When a flow control rule is configured for PPPoE packets on a port, the port permits only PPPoE packets matching the rule and drops any other packets.

NOTE:

When PPPoE flow control rules are configured on a port, all non-PPPoE packets are dropped.

On a PPPoE-agent-enabled switch, flow control rules take effect on all PPPoE packets except those transmitted at the discovery phase. If the PPPoE agent function is not enabled on a switch, the flow control rules take effect on all PPPoE packets.

Generally, the flow control rules are configured on the Ethernet ports connecting to PPPoE clients.

You can configure up to 16 PPPoE flow control rules on the port of an S3610 series Ethernet switch.

Examples

Configure a flow control rule on port Ethernet 1/0/1 to permit only PPPoE packets with source MAC address 0000-0000-0001 and destination MAC address 0000-0000-0002.

```
<H3C> system-view
[H3C] interface ethernet 1/0/1
[H3C-Ethernet1/0/1] traffic-pppoe source-address 0000-0000-0001 destination-address
0000-0000-0002
```

rule remark

Syntax

rule [*rule-id*] **remark** *text*

undo rule [*rule-id*] **remark** [*text*]

View

IPv4 basic/advanced ACL view, Ethernet frame header ACL view, User-defined ACL view

Default level

2: System level

Parameters

rule-id:

rule-id: Specifies a rule ID for the remark, in the range 0 to 65534. The rule ID determines the position of the remark. If no rule ID is provided, the system automatically assigns a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the remark is numbered 30.

text: Types a remark, a case sensitive string of 1 to 63 characters.

Description

Use the **rule remark** command to configure the start or end remark for a set of consecutive rules.

Use the **undo rule remark** command to delete the specified remark. If no rule ID is specified, all remarks are removed.

By default, no remarks are configured.

Examples

Display the rules in ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
#
```

```
return
```

To identify rules 10, 15, 20, and 25, add a start remark with rule ID 7, and an end remark with rule ID 27.

```
[Sysname-acl-basic-2000] rule 7 remark Rules for VIP_start
[Sysname-acl-basic-2000] rule 27 remark Rules for VIP_end
```

Display the rules in ACL 2000.

```
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 7 remark Rules for VIP_start
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
 rule 27 remark Rules for VIP_end
#
return
```

The output shows that the start remark is before rule 10, and the end remark is after rule 25. These two remarks clearly identify the purpose of the four rules.