
H3C S5500SI-CMW520-R2208

Release Notes

H3C S5500SI-CMW520-R2208 Release Notes

Keywords: Version Information, Version changed, Unresolved Problems and Avoidance Measures, List of Solved Problems.

Abstract: Provide all details about the application version file, include: Version Information, Version changed, Unresolved Problems and Avoidance Measures, List of Solved Problems.

Abbreviations:

Abbreviations	Full spelling
AAA	Authentication, Authorization and Accounting
ARP	Address Resolution Protocol
CMW	Comware
DHCP	Dynamic Host Configuration Protocol
GVRP	GARP VLAN Registration Protocol
IGMP	Internet Group Management Protocol
LACP	Link Aggregation Control Protocol
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network

Table of Contents

Version Information	6
Version Number	6
Chronological List of Version	6
Version Compatibility Table	7
Version Usage Limitations and Important Notes	8
Version Features	8
Version Hardware Features	8
Version Software Features	10
Version Changes	13
Changed Features	13
Changes in Command Lines	18
Changes in MIBs	29
Changes in Operations	33
S5500SI-CMW520- R2208 Changes in Operations	33
S5500SI-CMW520- F2206L12 Changes in Operations	33
S5500SI-CMW520- R2202P20 Changes in Operations	33
S5500SI-CMW520- R2202P19 Changes in Operations	33
S5500SI-CMW520- R2202P13 Changes in Operations	33
S5500SI-CMW520- R1208P03 Changes in Operations	33
S5500SI-CMW520- R1208P02 Changes in Operations	33
S5500SI-CMW520- R1208P01 Changes in Operations	34
S5500SI-CMW520- R1208 Changes in Operations	34
S5500SI-CMW520- R1207 Changes in Operations	34
S5500SI-CMW520- F1207 Changes in Operations	34
S5500SI-CMW520-R1205P03 Changes in Operations	34
S5500SI-CMW520- R1205P02 Changes in Operations	34
Unresolved Problems and Avoidance Measures	34
Resolved Problems	34
Resolved Problems in S5500SI-CMW520-R2208	34
Resolved Problems in S5500SI-CMW520-F2206L12	35
Resolved Problems in S5500SI-CMW520-R2202P20	36
Resolved Problems in S5500SI-CMW520-R2202P19	37
Resolved Problems in S5500SI-CMW520-R2202P13	37
Resolved Problems in S5500SI-CMW520-R2202P12	38
Resolved Problems in S5500SI-CMW520-R2202P11	38
Resolved Problems in S5500SI-CMW520-R2202P07	38
Resolved Problems in S5500SI-CMW520-R1208P03	39
Resolved Problems in S5500SI-CMW520-R1208P02	39
Resolved Problems in S5500SI-CMW520-R1208P01	39
Resolved Problems in S5500SI-CMW520-R1208	40

Resolved Problems in S5500SI-CMW520-R1207	41
Resolved Problems in S5500SI-CMW520-F1207.....	41
Resolved Problems in S5500SI-CMW520-R1205P03	42
Resolved Problems in S5500SI-CMW520-R1205P02	43
Documentation	46
Related Documentation.....	46
Online Technical Support.....	46
Software Upgrading	46
Introduction to Loading Modes	47
Local Software Loading.....	47
Boot Menu.....	47
Loading Software Using XModem Via Console Port.....	48
Loading Software Using TFTP Via Ethernet Port	53
Loading Software Using FTP Via Ethernet Port	54
Remote Software Loading	55
Remote Loading Using FTP.....	55
Remote Loading Using TFTP	57

List of Tables

Table 1 Version Information Table.....	6
Table 2 Version Compatibility Table	7
Table 3 S5500SI series switch Hardware Features	8
Table 4 S5500SI series switch Software Features	10
Table 5 Changed Features	13
Table 6 Changes in Commands	18
Table 7 Changes in MIB Files	29
Table 8 Related manuals	46
Table 9 Online technical support.....	46

Version Information

Version Number

Version Information: Comware software, Version 5.20, Release 2208

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

Chronological List of Version

Table 1 Version Information Table

Version Number	Based Version Number	Release Date	Remark
S5500SI-CMW520-R2208	S5500SI-CMW520-F2206L12	2010-12-27	
S5500SI-CMW520-F2206L12	S5500SI-CMW520-R2202P20	2010-08-27	
S5500SI-CMW520-R2202P20	S5500SI-CMW520-R2202P19	2010-05-28	
S5500SI-CMW520-R2202P19	S5500SI-CMW520-R2202P13	2010-02-25	
S5500SI-CMW520-R2202P13	S5500SI-CMW520-R2202P12	2009-10-30	
S5500SI-CMW520-R2202P12	S5500SI-CMW520-R2202P11	2009-09-30	
S5500SI-CMW520-R2202P11	S5500SI-CMW520-R2202P07	2009-09-02	
S5500SI-CMW520-R2202P07	S5500SI-CMW520-R1208P03	2009-07-30	
S5500SI-CMW520-R1208P03	S5500SI-CMW520-R1208P02	2009-06-30	
S5500SI-CMW520-R1208P02	S5500SI-CMW520-R1208P01	2009-04-30	
S5500SI-CMW520-R1208P01	S5500SI-CMW520-R1208	2009-03-30	
S5500SI-CMW520-R1208	S5500SI-CMW520-R1207	2009-02-25	
S5500SI-CMW520-R1207	S5500SI-CMW520-F1207	2007-12-18	
S5500SI-CMW520-F1207	S5500SI-CMW520-R1205P03	2007-09-24	
S5500SI-CMW520-R1205P03	S5500SI-CMW520-R1205P02	2007-04-18	
S5500SI-CMW520-R1205P02	S5500SI-CMW520-R1205	2007-01-30	
S5500SI-CMW520-R1205	First Release	2006-10-31	First time.

Version Compatibility Table

Table 2 Version Compatibility Table

Hardware Platform	S5500SI series
Equipment Model	H3C S5500-28C-SI/ H3C S5500-52C-SI/ H3C S5500-28C-PWR-SI/ H3C S5500-52C-PWR-SI H3C S5500-24P-SI/H3C S5500-48P-SI
Memory Requirement	128MB
Flash Requirement	16MB
Boot ROM Version	Version 603 or later(Note:This version number can be displayed by command display version under any view. Please see Note①)
Host Software	S5500SI-CMW520-R2208-S168.bin
iMC Version	iMC PLAT 3.20-R2606 + P13 + L15 iMC UAM 3.60-E6301 + P04 iMC EAD 3.60-E6301 + P04 iMC NTA 3.20-F0606 iMC QoS 3.20-F0606
iNode Version	iNode PC 3.60-E6307
Remark	S5500SI-CMW520-R2208-S168.bin is 168-bit encryption for SSH

Sample:To see the version number of the software and bootrom of the S5500SI Switch:

```
<H3C>dis ver
```

```
H3C Comware Platform Software
```

```
Comware Software, Version 5.20, Release 2208-----Note①
```

```
Copyright (c) 2004-2010 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
```

```
H3C S5500-28C-SI uptime is 0 week, 0 day, 7 hours, 28 minutes
```

```
H3C S5500-28C-SI with 1 Processor
```

```
128M bytes SDRAM
```

```
16384K bytes Flash Memory
```

```
Hardware Version is REV.A
```

```
CPLD Version is 007
```

```
Bootrom Version is 603-----Note②
```

```
[SubSlot 0] 24GE+4SFP Hardware Version is REV.A
```

Version Usage Limitations and Important Notes

1. VLAN ACLs cannot take effect on QinQ-enabled ports because of implementation limitations.
2. When the configuration of port isolation conflicts with the redirect action of QoS, the port isolation configuration overrides. For example, assume ports g1/0/1 and g1/0/2 belong to a port isolation group and the QoS policy applied on g1/0/1 contains a traffic behavior to redirect traffic received on g1/0/1 to g1/0/2. When receiving traffic matching the QoS policy, port g1/0/1 will not redirect it to port g1/0/2, because both ports are members of a port isolation group, which prevents them from forwarding traffic to each other.
3. The broadcast/multicast/unknown unicast suppression threshold configured as a percentage of the total bandwidth in port view is accurate only for 64-byte packets. This is because the chip supports only broadcast suppression by PPS, and the system converts the percentage into PPS per 64 bytes. Thus, you are recommended to configure storm suppression by PPS.
4. The virtual cable test (VCT) function will fail if the connected peer port works at 100 Mbps in forced mode.
5. Use the save option of the display diagnostic-information command to save diagnostic information to a file. The file is so large that the flash may not have enough space to save it. Thus the save operation fails.
6. Configure more than 5 VTY users in version R2208 or later, and upgrade it to R2202P21 or before. Then, restoring the configuration fails.

Version Features

Version Hardware Features

Table 3 S5500SI series switch Hardware Features

Item	Description						
	H3C S5500-28 C-SI	H3C S5500-52 C-SI	H3C S5500-2 8C-PW R-SI	H3C S5500-52 C-PWR-SI	H3C S5500-2 4P-SI	H3C S5500-4 8P-SI	
Dimensions (height × width × depth)	43.6 × 440 × 300 mm (1.72 × 11.8 × 17.3 in.)		43.6 × 440 × 260 mm (1.72 × 10.2 × 17.3 in.)		43.6 × 440 × 300 mm (1.72 × 11.8 × 17.3 in.)		
Weight	4 kg (8.1 lb)	4.5 kg (9.9 lb)	6 kg (13.2 lb)	6.5 kg (14.3 lb)	4 kg (8.1 lb)	4.5 kg (9.9 lb)	
Port Description	GE ports on the front panel	24 10/100/100M electrical ports	48 10/100/100M electrical ports	24 10/100/1000M electrical ports	48 10/100/100M electrical ports	24 10/100/1000M electrical ports	48 10/100/100M electrical ports
		4 Gigabit	4 Gigabit	4	4 Gigabit	4	4 Gigabit

		Description					
Item		H3C S5500-28 C-SI	H3C S5500-52 C-SI	H3C S5500-28C-PWR-SI	H3C S5500-52 C-PWR-SI	H3C S5500-24P-SI	H3C S5500-48P-SI
		SFP Combo ports	SFP Combo ports	Gigabit SFP Combo ports	SFP Combo ports	Gigabit SFP Combo ports	SFP Combo ports
Optional modules		1-port 10GE XFP module					
		2-port 10GE XFP module					
		2-port 10GE CX4 module for short haul		None			
		2-port 10GE SFP+ module					
		2-port GE SFP module					
Power supply	AC	Rated voltage: 100 VAC to 240 V AC, 50/60 Hz Input voltage: 90 VAC to 264 VAC, 47/63 Hz					
	DC	None		Rated voltage range: -52 VDC to 55 VDC	None		
Power consumption (full load)	80W	120W	455W: system power consumption 85 W and PoE power consumption 370 W	When an RPS is connected, full-load power consumption is 870 W including system power consumption 130 W and PoE power consumption 740 W.	62W	110W	
Operating temperature	0°C to 40°C						
Relative humidity (noncondensing)	10%~90%						

Version Software Features

Table 4 S5500SI series switch Software Features

Feature		S5500-28C-SI	S5500-24P-SI	S5500-52C-SI	S5500-48P-SI	S5500-28C-PWR-SI	S5500-52C-PWR-SI
Wire speed L2 switching	Switching capacity (Full duplex)	128 Gbps	48G bit/s	176 Gbps	96G bit/s	128 Gbps	176 Gbps
	Packet forwarding rate	95.2 Mpps	35.7Mpps	130.9 Mpps	71.4Mpps	95.2 Mpps	130.9 Mpps
Power over Ethernet		Not supported				Supported	
Link aggregation		<ul style="list-style-type: none"> • aggregation of GE ports • aggregation of 10-GE ports • Static link aggregation • Dynamic link aggregation • Supports local-first load sharing for link aggregation • Supports Configuring load sharing criteria for IRF links 					
IRF		<ul style="list-style-type: none"> • Intelligent Resilient Framework 					
IRF MAD Detection		<ul style="list-style-type: none"> • ARP MAD • LACP MAD 					
Flow control		IEEE 802.3x flow control and back pressure					
Jumbo Frame		Supports maximum frame size of 9 KB					
MAC address table		<ul style="list-style-type: none"> • 16K MAC addresses • 128 static MAC addresses • Blackhole MAC addresses • MAC address learning limit on a port 					
VLAN		<ul style="list-style-type: none"> • Port-based VLANs (4094 VLANs) • QinQ and selective QinQ • Voice VLAN • Protocol-based VLANs • MAC-based VLANs • IP subnet-based VLANs • GVRP • Isolate User Vlan 					
ARP		<ul style="list-style-type: none"> • 2K entries • 1K static entries • Gratuitous ARP • Standard proxy ARP and local proxy ARP • ARP source suppression • ARP detection (based on DHCP snooping entries/802.1x security entries/static IP-to-MAC bindings) • ARP Filter Binding 					
ND		<ul style="list-style-type: none"> • 1K entries 					

Feature	S5500-28C-SI	S5500-24P-SI	S5500-52C-SI	S5500-48P-SI	S5500-28C-PWR-SI	S5500-52C-PWR-SI
	<ul style="list-style-type: none"> • 512 static entries • ND Proxy • IPV6 ND Detection • IPV6 ND Snooping 					
VLAN virtual interface	64					
IPV4 DHCP	<ul style="list-style-type: none"> • DHCP Client • DHCP Snooping • DHCP Relay • DHCP Server 					
IPV6 DHCP	<ul style="list-style-type: none"> • IPV6 DHCP Snooping • PV6 DHCP Client • PV6 DHCP Relay • PV6 DHCP Server 					
UDP Helper	UDP Helper					
DNS	<ul style="list-style-type: none"> • Dynamic domain name resolution • Dynamic domain name resolution client • IPv4/IPv6 addresses 					
IPV4 route	<ul style="list-style-type: none"> • 64 static routes • RIP (Routing Information Protocol) v1/2; up to 512 IPv4 routes • Routing policy 					
IPV6 route	<ul style="list-style-type: none"> • 64static routes • RIPng; up to 256 IPv6 routes • Routing policy 					
IPV4 multicast	<ul style="list-style-type: none"> • IGMP (Internet Group Management Protocol) Snooping v1/v2/v3 • Multicast VLAN • Multicast VLAN+I 					
IPV6 multicast	<ul style="list-style-type: none"> • MLD Snooping v1/v2 • IPv6 multicast VLAN • IPv6 multicast VLAN+ 					
Broadcast/multicast/unicast storm control	<ul style="list-style-type: none"> • Storm control based on port rate percentage • PPS-based storm control 					
MSTP	<ul style="list-style-type: none"> • STP/RSTP/MSTP protocol • STP Root Guard • BPDU Guard 					
RRPP	<ul style="list-style-type: none"> • RRPP protocol • Multi-instance RRPP 					
Smart link	<ul style="list-style-type: none"> • Support Smart Link • Multi-instance Smart Link 					
Monitor link	Supported					
Bpdu tunnel	Cdp/dldp/oam/gvrp/hgmp/lacp/ldp/pagp/pvst/stp/udld/vtp					
QoS/ACL	<ul style="list-style-type: none"> • Restriction of the rates at which a port sends and receives packets, 					

Feature	S5500-28C-SI	S5500-24P-SI	S5500-52C-SI	S5500-48P-SI	S5500-28C-PWR-SI	S5500-52C-PWR-SI
	<ul style="list-style-type: none"> with a granularity of 64 kbps. • Packet redirection • Committed access rate (CAR), with a granularity of traffic limit 64 kbps. • Eight output queues for each port • Flexible queue scheduling algorithms based on port and queue, including strict priority (SP), weighted round robin (WRR), WFQ(Weighted Fair Queuing)and SP + WRR. • Remarking of 802.1p and DSCP priorities • Packet filtering at L2 (Layer 2) through L4 (Layer 4); flow classification based on source MAC address, destination MAC address, source IP (IPv4/IPv6) address, destination IP (IPv4/IPv6) address, port, protocol, and VLAN. • Time range • User Profile • Packet filter • Dynamic Modifying Qos 					
Mirroring	<ul style="list-style-type: none"> • Traffic mirroring • Port mirroring 					
Remote mirroring	Remote port mirroring					
Security	<ul style="list-style-type: none"> • Hierarchical management and password protection of users • AAA authentication • RADIUS authentication • HWTACACS • SSH 2.0 • Port isolation • Port security • MAC address authentication • IP-MAC-port binding(IPV4 and IPV6) • IP Source Guard • Https • SSL • PKI • EAD • Secure Local Area Network • Triple authentication 					
802.1X	<ul style="list-style-type: none"> • Up to 1,024 users • Port-based and MAC address-based authentication • Guest VLAN • Trunk port authentication • 802.1x-based dynamic QoS/ACL/VLAN delivery • 802.1x re-authentication • User Profile support Mac-authentication 					
Loading and upgrading	<ul style="list-style-type: none"> • Loading and upgrading through XModem protocol • Loading and upgrading through FTP 					

Feature	S5500-28C-SI	S5500-24P-SI	S5500-52C-SI	S5500-48P-SI	S5500-28C-PWR-SI	S5500-52C-PWR-SI
Management						
Maintenance						
Low Energy						

Version Changes

Changed Features

Table 5 Changed Features

Version Number	Item	Description
S5500SI-CMW520-R2208	Changed Hardware Features	New Features: add 2-port GE SFP module Deleted Features: None

Version Number	Item	Description
		<p>New Features:</p> <ul style="list-style-type: none"> • Configuring scheduled tasks; • Configuring the data buffer; • IRF MAD Detection: ARP MAD/LACP MAD; • Configuring temperature alarm thresholds for a member device; • Supports local-first load sharing for link aggregation; • Enabling link aggregation traffic redirection; • Supports Configuring load sharing criteria for IRF links; • Specifying the case (lowercase or uppercase) of usernames for MAC authentication; • Setting the aging time of sticky MAC addresses; • User Profile support Mac-authentication; • RSPAN mirror support reflect port; • QinQ VLAN transparent transmission; • ARP Filter Binding; • Configuring static multicast MAC address entries; • Configuring 802.1p precedence for IGMP messages; • Configuring 802.1p precedence for MLD messages; • Configuring IGMP Snooping Proxying; • Configuring MLD Snooping Proxying; • IPV6 Dhcp Snooping; • IPV6 ND Detection; • IPV6 ND Snooping; • User bind for IPV6; • IPV6 Dhcp Client; • IPV6 Dhcp Relay; • IPV6 Dhcp Server; • sFlow support configuring of IPV6 address ; • Unicast trigger function for 802.1X authentication; • Loopback-detection multiple port detection; • Loopback-detection can shutdown the detective port ; • ND Proxy; • Dynamic Modifying Qos; • Configuring dynamic MAC-based VLAN assignment; • Port auto-power-down; • Set the time after which a shut down BPDU guard port recovers; • Control the learning of DHCP snooping entries on trusted ports; <p>Deleted Features: None</p> <p>Modified Features:</p> <ul style="list-style-type: none"> • Modify VTY users from 5 to 16; • Modify the aggregation of 10-GE ports from 4 to 8; • Cfd support RFC;
	Changed Software Features	

Version Number	Item	Description
		<ul style="list-style-type: none"> Configuring the isolate-user-VLAN type for a port; ARP packet rate limit;
	Changed Hardware	New Features: Deleted Features: None
S5500SI-CMW 520-F2206L12	Changed Software Features	New Features: <ul style="list-style-type: none"> Triple Authentication Extended; portal user moving/ portal web-proxy/ portal offline-detect interval Multi-port Loopback Detection; Global Static IP Source Guard Binding; DHCP snooping supports QinQ; LACP Timeout Interval configuration; IRDP (ICMP Router Discovery Protocol); Layer 2 Isolation for Ports Within a Secondary VLAN; Deploy security authentication in the WiNet; Triple Authentication Feature; RMON2; Static Multicast MAC Address Configurable; MIB-IflIndex 32bit and 16bit switching ; DHCP Snooping Bindings Backup; IRF Multiple Radius Server Deleted Features: None Modified Features: None
S5500SI-CMW 520- R2202P20	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None
S5500SI-CMW 520- R2202P19	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: The command of ARP Quick Notify; Deleted Features: None Modified Features: None
S5500SI-CMW 520- R2202P13	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None
S5500SI-CMW 520-	Changed Hardware Features	New Features: None Deleted Features: None

Version Number	Item	Description
R2202P12	Changed Software Features	New Features: Configurable Mac-address of Each Port or Link aggregation; Deleted Features:None Modified Features: None
S5500SI-CMW 520-R2202P11	Changed Hardware Features	New Features: add H3C S5500-24P-SI/H3C S5500-48P-SI Deleted Features: None
	Changed Software Features	New Features:None Deleted Features:None Modified Features: None
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW 520-R2202P07	Changed Software Features	New Features: 802.1X Online User Handshake Security; MAC re-authenticate; Deleted Features: None Modified Features: None
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW 520-R1208P03	Changed Software Features	New Features: ACL Logging; LACP-MAD passthrough; Deleted Features: None Modified Features: None
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW 520-R1208P02	Changed Software Features	New Features: <ul style="list-style-type: none"> • 802.1x re-authentication; • MAC-address based Guest VLAN; • TACACS+ accounting; • The protocol of LLDP can get the physical port information according to the device name; • Bpdu tunnel; • the protocol of LACP marker; • configurable link aggregation load sharing by each link aggregation; • packet filter; Deleted Features: <ul style="list-style-type: none"> • Embedded Web-based network management; Modified Features: <ul style="list-style-type: none"> • modifying the "arp detection" mode change from "and" to "or";

Version Number	Item	Description
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW520-R1208P01	Changed Software Features	New Features: BPDU Dropping; Embedded Web-based network management; the command alias function; Deleted Features: None Modified Features: None
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW520-R1208	Changed Software Features	New Features: <ul style="list-style-type: none"> • Smart link; • Monitor link; • 802.1ag; • 802.3ah; • ARP detection; • ARP source suppression; • User profile; • Multiple voice VLAN; • LLDP; • DLDP; • Port security; • IP source guard; • sFlow; • Isolate-user VLAN; • RSPAN; • NQA; • Storm constrain; • Flow interval; • RRPP; • Subnet VLAN; • link aggregation load sharing configurable; Deleted Features: None Modified Features: <ul style="list-style-type: none"> • The Modification feature of Link aggregation • voice vlan support multiple vlan
S5500SI-CMW520-R1207	Changed Hardware Features	New Features: None Deleted Features: None
	Changed Software Features	New Features: None Deleted Features: None Modified Features: None
S5500SI-CMW520-F1207	Changed Hardware Features	New Features: None Deleted Features: None

Version Number	Item	Description
	Changed Software Features	New Features: IRF lite and EAD Deleted Features: None Modified Features: None
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW520-R1205P03	Changed Software Features	New Features: None Deleted Features: None Modified Features: 802.3ad is modified; Pure dynamic LACP mode is not supported, and only manual and static LACP modes are supported .
	Changed Hardware Features	New Features: None Deleted Features: None
S5500SI-CMW520-R1205P02	Changed Software Features	New Features: None Deleted Features: None Modified Features: None

Changes in Command Lines

Table 6 Changes in Commands

Version Number	Item	Description
	New Commands	Refer to H3C S5500-SI/EI Series Ethernet Switches Command References- Release 2208
S5500SI-CMW520-R2208	Deleted Commands	None
	Modified Commands	Refer to H3C S5500-SI/EI Series Ethernet Switches Command References- Release 2208
	New Commands	Refer to H3C S5500-SI/EI Series Ethernet Switches Command References- Release 2208
S5500SI-CMW520-F2206L12	Deleted Commands	None
	Modified Commands	The command used to display the summary information of an interface changes from display brief interface to display interface brief
	New Commands	None
S5500SI-CMW520-R2202P20	Deleted Commands	None
	Modified Commands	None
S5500SI-CMW5	New	mac address station move

Version Number	Item	Description
	Commands	Syntax mac-address station-move quick-notify enable undo mac-address station-move quick-notify enable View System view Default Level 2: System level Parameters None Description
20- R2202P19		Use the mac-address station-move quick-notify enable command to enable ARP quick notify. Use the undo mac-address station-move quick-notify enable command to restore the default. By default, ARP quick notify is disabled. Example <pre># Enable ARP quick notify. <Sysname> system-view [Sysname] mac-address station-move quick-notify enable</pre>
	Deleted Commands	None
	Modified Commands	None
	New Commands	None
S5500SI-CMW5 20- R2202P13	Deleted Commands	None
	Modified Commands	None
S5500SI-CMW5 20- R2202P12	New Commands	Mac-address Syntax mac-address mac-address undo mac-address View
		Layer 2 aggregate interface and Ethernet interface view Default Level 2: System level Parameters

Version Number	Item	Description
		<p>Layer 2 aggregate interface, ranging from 000f-e266-69c1 to 000f-e266-79c0.</p> <p>Description</p> <p>Use the mac-address command to assign a MAC address to the current Layer 2 aggregate interface.</p> <p>Use the undo mac-address command to restore the default.</p> <p>The default MAC address of a Layer 2 aggregate interface depends on your device model.</p> <p>notes</p> <p><i>By default, all aggregate interfaces on all S5500-SI series Ethernet switches have the same MAC address, and all Ethernet ports on an S5500-SI series Ethernet switch also have the same MAC address. For devices to communicate normally, you must ensure that:</i></p> <p><i>Different aggregate interfaces have different MAC addresses. To do that, you can use the mac-address command in aggregate interface view to change the MAC addresses of aggregate interfaces.</i></p> <p><i>Different member ports in a dynamic aggregation group have different MAC addresses. Before assigning an Ethernet port to a dynamic aggregation group, you may change its MAC address as needed. For how to configure the MAC address of an Ethernet port, see Ethernet Interface Configuration in the Access Volume.</i></p> <p>Examples</p> <pre># Assign MAC address 000f-e266-69c1 to Layer 2 aggregate interface Bridge-Aggregation 1. <Sysname> system-view [Sysname] interface bridge-Aggregation 1 [Sysname-Bridge-Aggregation-1] mac address 000f-e266-69c1</pre>
	Deleted Commands	None
	Modified Commands	None
	New Commands	None
S5500SI-CMW520-R2202P11	Deleted Commands	None
	Modified Commands	None
S5500SI-CMW520-R2202P07	New Commands	<ul style="list-style-type: none"> Command 1: 802.1X Online User Handshake Security <p>Syntax</p> <pre>dot1x handshake secure undo dot1x handshake secure</pre>

Version Number	Item	Description
		<p>View</p> <p>Ethernet Interface view</p> <p>Default Level</p> <p>System level</p> <p>Parameters</p> <p>None</p> <p>Description</p> <p>Use the dot1x handshake secure command to enable the online user handshake security function so that the device can prevent users from using illegal client software.</p> <p>Use the undo dot1x handshake secure command to disable the function.</p> <p>By default, the function is disabled.</p> <p>Note that:</p> <p><i>The online user handshake security function is implemented based on the online user handshake function. To bring the security function into effect, keep the online user handshake function enabled.</i></p> <p><i>The iNode client software and iMC server are recommended to ensure the normal operation of the online user handshake security function.</i></p> <p>Related commands: dot1x handshake.</p>
	Deleted Commands	None
	Modified Commands	None

S5500SI-CMW5
20- R1208P03

New
Commands

- Command 1:ACL Logging

[Syntax](#)

acl logging frequency frequency

undo acl logging frequency

[View](#)

System view

[Description](#)

Use the **acl logging frequency** command to set the interval for IPv4 packet filtering statistics. At the specified interval, the device outputs the statistics information, including the number of filtered packets, and the ACL rules used.

Use the **undo acl logging frequency** command to restore the default.

Version Number	Item	Description
		<p>Syntax</p> <p>acl ipv6 logging frequency <i>frequency</i></p> <p>undo acl ipv6 logging frequency</p> <p>View</p> <p>System view</p> <p>Description</p> <p>Use the acl ipv6 logging frequency command to set the interval for IPv6 packet filtering statistics. At the specified interval, the device outputs the statistics information, including the number of filtered packets, and the ACL rules used.</p> <p>Use the undo ipv6 acl logging frequency command to restore the default.</p> <p>By default, the interval is 0, that is, no IPv6 packet filtering statistics is collected.</p>
	Deleted Commands	None
S5500SI-CMW520- R1208P02	Modified Commands	None

New
Commands

- Command 1: 802.1x re-authentication

[Syntax](#)

dot1x re-authenticate

undo dot1x re-authenticate

[View](#)

Ethernet interface view

[Description](#)

Use the **dot1x re-authenticate** command to enable the periodic re-authentication function.

Use the **undo dot1x re-authenticate** command to restore the default.

- Command 2: 802.1x re-authentication

[Syntax](#)

dot1x timer reauth-period *reauth-period-value*

undo dot1x timer reauth-period

Version Number	Item	Description
		<ul style="list-style-type: none"> Command 3: MAC-address based Guest VLAN <p>Syntax</p> <p>mac-authentication guest-vlan <i>guest-vlan-id</i> undo mac-authentication guest-vlan</p> <p>View</p> <p>Layer 2 Ethernet interface view</p> <p>Description</p> <p>Use the mac-authentication guest-vlan command to specify a MAC-based guest VLAN (MGV) for MAC authentication. After the configured MGV takes effect, all users failing the authentication on the port will be added to the guest VLAN.</p> <p>Use the undo mac-authentication guest-vlan command to remove the guest VLAN configuration.</p> <ul style="list-style-type: none"> Command 4: TACACS+ accounting <p>Syntax</p> <p>accounting command hwtacacs-scheme <i>hwtacacs-scheme-name</i> undo accounting command</p> <p>View</p> <p>ISP domain view</p> <p>Description</p> <p>Use the accounting command command to specify the HWTACACS scheme for command line users.</p> <p>Use the undo accounting command command to restore the default.</p> <ul style="list-style-type: none"> Command 5: TACACS+ accounting <p>Syntax</p> <p>command accounting undo command accounting</p> <p>View</p> <p>User interface view</p> <p>Description</p> <p>Use the command accounting command to enable command accounting.</p> <p>Use the undo command accounting command to restore the default.</p> <ul style="list-style-type: none"> Command 6: TACACS+ accounting <p>Syntax</p>

Version Number	Item	Description
		<p>command authorization</p> <p>undo command authorization</p> <p>View</p> <p>User interface view</p> <p>Description</p> <p>Use the command authorization command to enable command authorization.</p> <p>Use the undo command authorization command to restore the default.</p> <ul style="list-style-type: none"> Command 7: The protocol of LLDP can get the physical port information according to the device name <p>Syntax</p> <p>display lldp neighbor-information [brief interface <i>interface-type interface-number</i> [brief]] list [system-name <i>system-name</i>]]</p> <p>View</p> <p>Any view</p> <p>Description</p> <p>Use the display lldp neighbor-information command to display the LLDP information about the neighboring devices received on the local device. The LLDP information is sent as TLVs.</p> <ul style="list-style-type: none"> Command 8: Bpdu tunnel <p>Syntax</p> <p>In Ethernet interface view or port group view:</p> <p>bpdu-tunnel dot1q { cdp dldp eoam gvrp hgmp lACP lldp pagp pvst stp udld vtp }</p> <p>undo bpdu-tunnel dot1q { cdp dldp eoam gvrp hgmp lACP lldp pagp pvst stp udld vtp }</p> <p>In Layer 2 aggregate interface view:</p> <p>bpdu-tunnel dot1q { cdp gvrp hgmp pvst stp vtp }</p> <p>undo bpdu-tunnel dot1q { cdp gvrp hgmp pvst stp vtp }</p> <p>View</p> <p>Ethernet interface view, Layer 2 aggregate interface view, port group view</p> <p>Description</p> <p>Use the bpdu-tunnel dot1q command to enable BPDU tunneling for a protocol on the current port or ports.</p>

Version Number	Item	Description
		<p>Use the undo bpdu-tunnel dot1q command to disable BPDU tunneling for a protocol on the port or ports.</p> <ul style="list-style-type: none"> Command 9: configurable link aggregation load sharing by each link aggregation <p>Syntax</p> <p>link-aggregation load-sharing mode { destination-ip destination-mac source-ip source-mac } *</p> <p>undo link-aggregation load-sharing mode</p> <p>View</p> <p>Layer 2 aggregate interface view</p> <p>Description</p> <p>Use the link-aggregation load-sharing mode command to configure the aggregation group-specific link aggregation load sharing mode.</p> <ul style="list-style-type: none"> Command 10: packet filter <p>Syntax</p> <p>packet-filter { <i>acl-number</i> name <i>acl-name</i> } { inbound }</p> <p>undo packet-filter { <i>acl-number</i> name <i>acl-name</i> } { inbound }</p> <p>View</p> <p>Ethernet interface view, VLAN interface view</p> <p>Description</p> <p>Use the packet-filter command to apply an ACL to an interface to filter IPv4 packets or Ethernet frames.</p> <p>Use the undo packet-filter command to restore the default.</p> <ul style="list-style-type: none"> Command 11: packet filter <p>Syntax</p> <p>packet-filter ipv6 { <i>acl6-number</i> name <i>acl6-name</i> } { inbound }</p> <p>undo packet-filter ipv6 { <i>acl6-number</i> name <i>acl6-name</i> } { inbound }</p> <p>View</p> <p>Ethernet interface view, VLAN interface view</p> <p>Description</p> <p>Use the packet-filter ipv6 command to apply a basic or advanced IPv6 ACL to an interface to filter IPv6 packets.</p> <p>Use the undo packet-filter ipv6 command to restore the default.</p>
	Deleted	<ul style="list-style-type: none"> Command 1: packet filter

Version Number	Item	Description
	Commands	<p>Syntax</p> <p>port interface-list</p> <p>undo port interface-list</p> <p>View</p> <p>VLAN view</p> <p>Description</p> <p>Use the port command to assign the specified access port(s) to the current VLAN.</p> <p>Use the undo port command to remove the specified access port(s) from the current VLAN.</p> <p>Explain</p> <p><i>Interface-list</i>: not support the Layer 2 aggregate interface list any more.</p> <hr/> <ul style="list-style-type: none"> Command 1: <p>Syntax</p> <p>arp detection mode { dhcp-snooping dot1x static-bind }</p> <p>undo arp detection mode { dhcp-snooping dot1x static-bind }</p> <p>View</p> <p>System view</p> <p>Description</p> <p>Use the arp detection mode command to specify an ARP attack detection mode.</p> <p>Use the undo arp detection mode command to cancel the specified ARP detection mode.</p> <p>Explain</p> <p>The "arp detection" mode change from "and" to "or".</p> <hr/>
S5500SI-CMW520-R1208P01	Modified Commands	<hr/> <ul style="list-style-type: none"> Command 1:BPDU Dropping <p>Syntax</p> <p>bpdu-drop any</p> <p>undo bpdu-drop any</p> <p>View</p> <p>Ethernet interface view, port group view, Layer-2 aggregate interface view</p> <p>Description</p> <p>Use the bpdu-drop any command to enable BPDU dropping</p>
	New Commands	<ul style="list-style-type: none"> Command 1:BPDU Dropping <p>Syntax</p> <p>bpdu-drop any</p> <p>undo bpdu-drop any</p> <p>View</p> <p>Ethernet interface view, port group view, Layer-2 aggregate interface view</p> <p>Description</p> <p>Use the bpdu-drop any command to enable BPDU dropping</p>

Version Number	Item	Description
		dropping on the Ethernet port.
		<ul style="list-style-type: none"> Command 2:The command alias function <p>Syntax</p> <p>command-alias enable undo command-alias enable</p> <p>View</p> <p>System view</p> <p>Description</p> <p>Use the command-alias enable command to enable the command alias function.</p> <p>Use the undo command-alias enable command to disable the command alias function.</p>
		<ul style="list-style-type: none"> Command 3:The command alias function <p>Syntax</p> <p>command-alias mapping <i>cmdkey alias</i> undo command-alias mapping <i>cmdkey</i></p> <p>View</p> <p>System view</p> <p>Description</p> <p>Use the command-alias mapping command to configure command aliases.</p> <p>Use the undo command-alias mapping command to delete command aliases.</p>
		<ul style="list-style-type: none"> Command 4:The command alias function <p>Syntax</p> <p>display command-alias</p> <p>View</p> <p>Any view</p> <p>Description</p> <p>Use the display command-alias command to display defined command aliases and the corresponding commands.</p>
	Deleted Commands	None
S5500SI-CMW520- R1208	Modified Commands	None

Version Number	Item	Description
		H3C S5500-SI Series Ethernet Switches Command Manual-Release 1208
	Deleted Commands	None
S5500SI-CMW520- R1207	Modified Commands	For link aggregation configuration commands, refer to: H3C S5500-SI Series Ethernet Switches Operation Manual-Release 1208 H3C S5500-SI Series Ethernet Switches Command Manual-Release 1208
	New Commands	None
	Deleted Commands	None
S5500SI-CMW520- F1207	Modified Commands	<p>qos car inbound { any acl { [ipv6] INTEGER<0-4294967295> INTEGER<4000-4999> } } cir INTEGER<0-4294967295> [cbs INTEGER<0-4294967295> [ebs INTEGER<0-4294967295>]] [pir INTEGER<0-4294967295>] [green { pass discard remark-prec-continue INTEGER<0-7> remark-dscp-continue STRING<1-31> remark-dot1p-continue INTEGER<0-7> }] [red { discard pass remark-dscp-continue STRING<1-31> }]</p> <p>is modified as follow:</p> <p>qos car inbound { any acl { [ipv6] INTEGER<0-4294967295> INTEGER<4000-4999> } } cir INTEGER<0-4294967295> [cbs INTEGER<0-4294967295> [ebs INTEGER<0-4294967295>]] [pir INTEGER<0-4294967295>] [green { pass discard remark-dscp-continue STRING<1-31> }] [red { discard pass remark-dscp-continue STRING<1-31> }].</p> <p>Delete remark-prec-continue and remark-dot1p-continue behavior of green packet.</p>
	New Commands	Please refer to Chinese document
	Deleted Commands	None
S5500SI-CMW520- R1205P03	Modified Commands	None
	New Commands	None
	Deleted Commands	Deleted Command: [H3C-GigabitEthernet1/0/1]lACP enable [H3C-GigabitEthernet1/0/1]undo lACP enable Specification: the Mode of 'Static' also run LACP, and can replace Pure Dynamic LACP mode.
S5500SI-CMW520- R1205P02	Modified Commands	None
	New Commands	mac-authentication user-name-format mac-address [with-hyphen without-hyphen]. specify the format of MAC addresses as usernames and passwords with-hyphen or

Version Number	Item	Description
		without-hyphen; mac-authentication user-name-format fixed [account STRING<1-55>] [password { simple STRING<1-256> cipher STRING<1-256> }]; specify the centralized MAC address authentication mode as fixed mode; undo mac-authentication user-name-format: Restore the default centralized MAC address authentication mode.
	Deleted Commands	None

Changes in MIBs

Table 7 Changes in MIB Files

Version Number	Item	MIB File Name	Module Name	Description
S5500SI-CM W520-R2208	New	None		<ul style="list-style-type: none"> • Add H3C-DHCP-SERVER-MIB. • Added DOT3-OAM-MIB and IEEE8021-CFM-MIB; • Added hh3cEntityExtLowerTemperatureThreshold, hh3cEntityExtShutdownTemperatureThreshoId and hh3cEntityExtTemperatureLower, hh3cEntityExtTemperatureTooUp, hh3cEntityExtTemperatureNormal; • Added hh3cRadiusAuthServerTable to HH3C-RADIUS-MIB; • Added hh3cDomainCurrentAccessNum to hh3cDomainInfoTable ; • Added hh3cCBQoSNEstPolicyCfGInfoTable and hh3cCBQoSNEstPolicyApplyObjectTable in HH3C-CBQOS2-MIB; • Added RFC4133-MIB and RFC4022-MIB; • Added hh3cRadiusAuthErrThredshold in HH3C-RADIUS-MIB; • Added hh3cDHCPserverAvgIpUseThreshold, hh3cDHCPserverMaxIpUseThreshold, hh3cDHCPserverAllocateThreshold in hh3cDHCPserverObjects in HH3C-DHCP-SERVER-MIB; • Add SubCard of "LSPM2GP2P" in the entPhysicalModelName;
	Modified	None		<ul style="list-style-type: none"> • Modified description of dot1xPaePortReauthenticate, dot1xAuthReAuthPeriod, dot1xAuthReAuthEnabled and

Version Number	Item	MIB File Name	Module Name	Description
				hh3cdot1xAuthReAuthPeriod ; <ul style="list-style-type: none"> Modified description of hh3cEntityExtTemperature, hh3cEntityExtTemperatureThreshold, hh3cEntityExtCriticalTemperatureThreshold, hh3cdevMSlotEnvironmentType, hh3cDevMSlotEnvironmentStatus and hh3cDevMSlotEnvironmentValue ; Modified description of hh3cMaxMacLearn ; Modify the description of Board in entPhysicalSoftwareRev; Modified description of hh3cEntityExtTemperature; Modified description of hh3cSysReloadSchedule; Modified description of hh3cRrppDomainInstanceListLow, hh3cRrppDomainInstanceListHigh, hh3cRrppDomainProtectVlanListLow and hh3cRrppDomainProtectVlanListHigh.
	New	None		<ul style="list-style-type: none"> Added H3C-CBQOS2-MIB;
S5500SI-CM W520-F2206L 12	Modified	None		<ul style="list-style-type: none"> Modify description of dot1xPaePortReauthenticate in IEEE8021-PAE-MIB; Modify description of h3cDLDPAuthenticationPassword in H3C-DLDP-MIB; Modified description of h3cEntityExtTemperature in H3C-ENTITY-EXT-MIB;
S5500SI-CM W520-R2202 P20	New	None		None
	Modified	None		None
S5500SI-CM W520-R2202 P19	New	None		None
	Modified	None		None
S5500SI-CM W520-R2202 P13	New	None		None
	Modified	None		None
S5500SI-CM W520-R2202 P12	New	None		None
	Modified	None		None
	New	None		None
S5500SI-CM W520-R2202 P11	Modified	Reference Description		Modify sysObjectID in RFC 1213 mib
S5500SI-CM	New	None		None

Version Number	Item	MIB File Name	Module Name	Description
W520-R2202 P07	Modified	None		None
S5500SI-CM W520-R1208 P03	New	None		None
	Modified	None		None
	New	None		None
S5500SI-CM W520-R1208 P02	Modified	Reference Description		Modify dot1xPaePortTable of dot1xPaeSystem in IEEE8021X MIB ;
S5500SI-CM W520-R1208 P01	New	None		None
	Modified	None		None
	New	Reference Description		<ul style="list-style-type: none"> Added H3C-CBOOS2-MIB, H3C-QOS-CAPABILITY-MIB. Added h3cEntityExtSFPPPhony to common traps in the H3C-ENTITY-EXT-MIB Added h3cExpirationDate, h3cUserGroup and h3cUserGroupInfoTable in the H3C-USER-MIB Added hwdot1xAuthMethod in hwdot1xPaeSystem group in the IEEE8021X MIB. Added hwlmgmpSnoopingNonFloodingStatus, hwlmgmpSnoopingStatsObjects, hwlmgmpSnoopingVlanStatusTable in the HUAWEI-LswIGSP-MIB. Added Scalar Objects in H3C-UI-MAN-MIB Added h3cSysCurBtmFileName and h3cSysCurUpdateBtmFileName in the H3C-SYS-MAN-MIB. Added h3cProcessTable in H3C-ENTITY-EXT-MIB Add H3C-MAC-INFORMATION-MIB.
S5500SI-CM W520-R1208	Modified	Reference Description		<ul style="list-style-type: none"> Modified description of h3cUserName in the H3C-USER-MIB modified details of ipv6lfDescr in the IPV6-MIB; modified description of h3cQinQProtocolIndex and h3cQinQBpduTunnelSwitch in the H3C-QINQ-MIB; Modified description of pingCtlDescr in the DISMAN-PING-MIB; Modified description of hwdot1qVlanIpAddress, hwdot1qVlanIpAddressMask in the HUAWEI-LswVLAN-MIB; modified description of h3cUserIndex in the

Version Number	Item	MIB File Name	Module Name	Description
				H3C-USER-MIB <ul style="list-style-type: none"> Modified description of h3cRdAccRealTime in the H3C-RADIUS-MIB; Update H3C-RRPP-MIB; Modified description of h3cIdleCut in the H3C-USER-MIB; Modified description of ot3adAggTable and hwAggLinkTable in the H3C-USER-MIB; Modified description of h3cCfgRunModifiedLast in the H3C-CONFIG-MAN-MIB. Modified description of hwNTPPeerRowStatus in the H3C-NTP-MIB Modified PDS of h3cRdPrimState, h3cRdSecState, h3cRdPrimAccState, h3cRdSecAccState in the H3C-RADIUS-MIB Modified the description of h3cVoiceVlanEnabledId and h3cVoiceVlanPortEnableList in the H3C-VOICE-VLAN-MIB Modified description of H3C-SYS-MAN-MIB. Modified description of eventDescription in the RMON-MIB Modified DISMAN-PING-MIB, H3C-NQA-MIB and HUAWEI-DISMAN-PING-MIB Modified description of h3cCfgLogTable in the H3C-CONFIG-MAN-MIB Modified description of hwdot1qTpFdbSetOperate in the HUAWEI-LswMAM-MIB Modified description of H3cFlashOperationStatus in the H3C-FLASH-MAN-MIB
S5500SI-CM W520-R1207	New	None		
	Modified	None		
S5500SI-CM W520-F1207	New	None		
	Modified	None		
	New	None		
S5500SI-CM W520-R1205 P03	Modified	Reference Description		<ul style="list-style-type: none"> Modify sysContact to "Hangzhou H3C Tech. Co.,Ltd." In the RFC1213-MIB Modify sysLocation to "Hangzhou, China" In the RFC1213-MIB
S5500SI-CM W520-R1205 P02	New	None		
	Modified	None		

Changes in Operations

S5500SI-CMW520- R2208 Changes in Operations

The default load balance for link aggregation is local-first load sharing.

S5500SI-CMW520- F2206L12 Changes in Operations

1. The command used to display the summary information of an interface changes from **display brief interface** to **display interface brief**;
2. When the DHCP server and client are on the same subnet: With the keyword `subaddress` specified, the DHCP server will preferably assign an IP address from an address pool that resides on the same network segment as the primary IP address of the server interface (connecting the client). If the address pool contains no assignable IP address, the server assigns an IP address from an address pool that resides on the same network segment as the secondary IP addresses of the server interface. If the interface has multiple secondary IP addresses, the server first assigns an IP address from an address pool that contains the firstly configured secondary IP address. If the address pool contains no assignable IP address, the server assigns one from an address pool that contains the secondly configured secondary IP address. Without the keyword `subaddress` specified, the DHCP server can only assign an IP address from the address pool that resides on the same network segment as the primary IP address of the server interface.
3. In a version before F2206L12, after a mapping between an Isolate-user-VLAN and Secondary VLAN is configured, the ports in the Isolate-user-VLAN automatically join the Secondary VLAN, and the ports in the Secondary VLAN automatically join the Isolate-user-VLAN. In version F2206L12 or a later version, to enable the automatic join function, you must configure the **port isolate-user-vlan promiscuous** command on the ports in the Isolate-user-VLAN, and the **port isolate-user-vlan host** command on the ports in the Secondary VLAN before configuring the mapping.

S5500SI-CMW520- R2202P20 Changes in Operations

None.

S5500SI-CMW520- R2202P19 Changes in Operations

"IRF Lite" can work on GE port.

S5500SI-CMW520- R2202P13 Changes in Operations

None.

S5500SI-CMW520- R1208P03 Changes in Operations

modifying the IGMP-Snooping and MLD-Snooping multicast groups from 128 to 1000.

S5500SI-CMW520- R1208P02 Changes in Operations

The arp detection { dhcp-snooping | dot1x | static-bind } three mode relationship change from "and" to "or", then one of three pass the security check will be successful.

S5500SI-CMW520- R1208P01 Changes in Operations

None.

S5500SI-CMW520- R1208 Changes in Operations

The configuration of "Voice VLAN" can't be compatible with the last Version, and WEB can't support configuring the function of "Voice VLAN".

S5500SI-CMW520- R1207 Changes in Operations

None.

S5500SI-CMW520- F1207 Changes in Operations

None.

S5500SI-CMW520-R1205P03 Changes in Operations

None.

S5500SI-CMW520- R1205P02 Changes in Operations

None.

Unresolved Problems and Avoidance Measures

LSD55540

First found-in version: S5500SI-CMW520-R2208

Description: Change the PVID of an access port where some local users have passed MAC authentication. The authenticated users cannot be added to the new VLAN, and their communications are interrupted.

Workarounds: None.

Resolved Problems

Resolved Problems in S5500SI-CMW520-R2208

LSD52619

First found-in version: S5500SI-CMW520-F2206L12

Condition: Two or more devices form an IRF virtual device. Then telnet to the IRF virtual device and execute the display diagnostic-information command.

Description: All the IRF member devices reboot.

LSD52545

First found-in version: S5500SI-CMW520-F2206L12

Condition: Two or more devices form an IRF virtual device. When the IRF virtual device has learned 2000 ARP entries and has more than 200M Layer-3 traffic to forward, reboot the master.

Description: Some slave devices generate memory alarms and then reboot.

LSD54777

First found-in version: S5500SI-CMW520-F2206L12

Condition: Enable DHCP snooping and IP check on an IRF virtual device. When multiple DHCP clients are online, performing an IRF master/slave switchover.

Description: The devices work abnormally

HWD23534

First found-in version: S5500SI-CMW520-R1208

Condition: The temperature of an optical module is subzero.

Description: The temperature information of the optical module displayed at the CLI is incorrect.

HWD23536

First found-in version: S5500SI-CMW520-R1208

Condition: Display the optical power information of an optical module at the CLI.

Description: The displayed information is incorrect.

LSD51999

First found-in version: S5500SI-CMW520-R1208

Conditions: Enable sFlow.

Description: If the output port of the sampled packets is unknown, the device fills the egress port field with all 1s.

LSD51697

First found-in version: S5500SI -CMW520-F2206L12

Condition: In Layer-2 aggregate port view, configure the hybrid link type and the default VLAN. Then configure the port to allow packets tagged with the default VLAN to pass.

Description: The configuration fails.

Resolved Problems in S5500SI-CMW520-F2206L12

LSD35368

First found-in version: S5500SI-CMW520-R1208

Condition: Log into the web interface, then choose the View of "Qos".

Description: Disable traffic redirection. But the operation does not take effect.

LSD44792

First found-in version: S5500SI-CMW520-R1208

Condition: Delete the default voice VLAN OUI address of the device.

Description: The device still modifies the priorities of packets whose source MAC address is the deleted OUI address.

LSD48053

First found-in version: S5500SI-CMW520-R1208

Condition: Enable loopback-detection on the device.

Description: The configured loopback-detection interval-time is not applied correctly. The actually applied value is 40 percent of the configured value.

LSD51011

First found-in version: S5500SI-CMW520-R1208

Condition: Insert a GE line card and then insert an optical module into the GE line card. After that, ping or telnet to a VLAN interface of the switch through any port.

Description: Packet loss occurs.

LSD48997

First found-in version: S5500SI-CMW520-R1208

Condition: Configure Triple authentication. A MAC authentication client is moved from a switch port to another, and then performs MAC authentication.

Description: MAC authentication fails.

Resolved Problems in S5500SI-CMW520-R2202P20

LSD46280

First found-in version: S5500SI-CMW520-R1208

Condition: Disable "bootrom password recovery" in the Boot Menu.

Description: The super password in the configuration file does not take effect after reboot.

LSD48254

First found-in version: S5500SI-CMW520-R1208

Condition: Configure ip forward-broadcast and UDP-Helper on two virtual interfaces.

Description: UDP Packets are forwarded within the device until TTL=0.

LSD48159

First found-in version: S5500SI-CMW520-R1208

Condition: Configure a switch as a DHCP relay agent that forwards "bootstrap protocol" of DHCP DISCOVER packets that have a length less than 300 bytes from DHCP clients to the DHCP server.

Description: The DHCP server discards such packets because their lengths are less than 300 bytes.

Resolved Problems in S5500SI-CMW520-R2202P19

LSD43032

First found-in version: S5500SI-CMW520-R1208

Condition: A device is configured as a DHCP relay agent that stores two client entries with the same IP address.

Description: Lease operations for that IP address through the relay agent will fail.

LSD43608

First found-in version: S5500SI-CMW520-R1208

Condition: Enable DHCP snooping on a device with an aggregate port as the down link.

Description: DHCP discovery and request packets received from the aggregate port are discarded.

LSD44509

First found-in version: S5500SI-CMW520-R1208

Condition: Configure storm-constrain on multiple ports. Then, the storm-constrain limit on one of these ports is reached.

Description: All these ports take control actions.

LSD45422

First found-in version: S5500SI-CMW520-R1208

Condition: Plug an SFP plus cable of H3C into an H3C device.

Description: The SFP plus cable cannot be identified as an H3C cable.

LSD45783

First found-in version: S5500SI-CMW520-R1208

Condition: Read the dot1qTpFdbPort node.

Description: The returned value is wrong.

Resolved Problems in S5500SI-CMW520-R2202P13

LSD42808

First found-in version: S5500SI-CMW520-R1208

Condition: Configure DHCP snooping on a device. A DHCP snooping trusted port on the device receives a DHCP discovery and then a DHCP request packet. After that,if the port receives a DHCP offer or DHCP ACK packet.

Description: The packet is forwarded through the receiving port.

Resolved Problems in S5500SI-CMW520-R2202P12

ZDTB00157

First found-in version: S5500SI-CMW520-R1208

Condition: Enable LLDP on a port. The VLANs to which the port belongs have no management address configured.

Description: The management address filled in the LLDP packets is 127.0.0.1.

LSD42433

First found-in version: S5500SI-CMW520-R1208

Condition: Connect a device to a huawei's device (such as Quidway NE or Quidway 5300), and run LLDP between them.

Description: The LLDP neighbor cannot be found.

Resolved Problems in S5500SI-CMW520-R2202P11

None

Resolved Problems in S5500SI-CMW520-R2202P07

LSD41220

First found-in version: S5500SI-CMW520-R1208

Condition: Read the dot3adAggEntry mib node.

Description: A wrong value that the NMS cannot identify is returned.

LSD40942

First found-in version: S5500SI-CMW520-R1208

Condition: Connect a device to a CISCO device, and run LACP between them, and then add or remove VLANs on the device.

Description: The aggregation member ports on the CISCO device go down.

LSD40759

First found-in version: S5500SI-CMW520-R1208

Condition: A running device obtains and saves a local certificate and then restarts.

Description: After restart, the local certificate cannot recover, and consequently the functions using the certificate cannot work.

LSD40929

First found-in version: S5500SI-CMW520-R1208

Condition: A devices uses a certificate of a certificate chain that has three or more certificates.

Description: Using HTTPS to log in to the device causes it to reboot.

Resolved Problems in S5500SI-CMW520-R1208P03

LSD38359

First found-in version: S5500SI-CMW520-R1208P02

Condition: A BPDU tunnel interface on the device receives PVST packets tagged with VLANs that are inexistent on the device.

Description: Such PVST packets cannot be encapsulated/de-encapsulated normally.

LSD38221

First found-in version: S5500SI-CMW520-R1208P02

Condition: Add a BPDU tunnel interface to a link aggregation group and then change the state of the link aggregation group from inactive to active.

Description: There is little probability that the BPDU tunnel interface cannot process received STP packets normally.

LSD39122

First found-in version: S5500SI-CMW520-R1208P02

Condition: Run SNMP on S5500SI devices.

Description: These devices have the same SNMP local engine ID.

Resolved Problems in S5500SI-CMW520-R1208P02

LSD37931

First found-in version:S5500SI-CMW520-R1208P01

Condition: The device has both DHCP snooping and DHCP relay agent enabled.

Description: no record in DHCP-snooping.

Resolved Problems in S5500SI-CMW520-R1208P01

LSD36550

First found-in version: S5500SI-CMW520-R1208

Condition: Insert an RPS power supply into the device.

Description: The web interface displays the power input type of the RPS power supply as AC, which is DC in fact.

LSD37416

First found-in version: S5500SI-CMW520-R1208

Condition: Log out the CLI through the console port and log in to the web interface. Select "Cluster" ->"Setup"->" Build a cluster and to be commander" and configure parameters on the page.

Description: Click **Apply**. The device reboots.

LSD36607

First found-in version: S5500SI-CMW520-R1208

Condition: The device acts as an NTP client.

Description: After the device runs for a while, NTP synchronization fails.

Resolved Problems in S5500SI-CMW520-R1208

LSD24351

First Found-in Version: S5500SI-CMW520-R1207

Conditions: After system setting up

Symptoms: The Device should enable Cluster default, Panel Led should display 'c' due to the device as a candidate member of the Cluster ,and Panel Led display '1' in the condition of the Device disable the Cluster.

LSD20992

First Found-in Version: S5500SI-CMW520-F1207

Conditions: **stack ip-pool** configured firstly, then if you configure the **stack role master** command and then cancel the configuration.

Symptoms: **stack ip-pool** configured previously will become **cluster ip-pool** in the configuration.

LSD22347

First Found-in Version: S5500SI-CMW520-F1207

Conditions: When a 10GE card is inserted into the Device.

Symptoms: The cable type of a 10GE port is displayed as **Not Support** on the Web interface. Besides, after the cable type of a 10GE port is set to **Auto**, it is displayed as **Normal**.

LSD22875

First Found-in Version: S5500SI-CMW520-F1207

Conditions: In the case that the device connects to multiple users through multiple ports, STP surges, users repeatedly join/leave the multicast group, and 802.1x users log in/off repeatedly.

Symptoms: The device memory leak may occur to the 512-byte memory of the 0822 module on the Device.

Resolved Problems in S5500SI-CMW520-R1207

LSD18588

First Found-in Version: S5500SI-CMW520-F1207

Conditions: Enable 802.1x and EAD in system view of the device, enable 802.1x on the Combo electrical port, and then switch to the Combo optical port.

Symptoms: Because the ACL deny rule of the EAD applied on the Combo electrical port is not deleted, the device cannot be pinged through the Combo optical port.

LSD17237

First Found-in Version: S5500SI-CMW520-F1207

Conditions: Add or delete MAC addresses for many many times.

Symptoms: A MAC address cannot be deleted and a fail result is returned at each delete operation. However, this problem happens at a small probability.

Resolved Problems in S5500SI-CMW520-F1207

LSD10368

First Found-in Version: S5500SI-CMW520-R1205

Condition: When configuring link-aggregation and IGMP-snooping static-group and host-join on the port of expansion module.

Description: Hot-swap of the expansion module may cause some multicast groups traffic lost.

LSD10396

First Found-in Version: S5500SI-CMW520-R1205

Condition: None

Description: Xmodem command is missing in CLI, so that user can not use the Xmodem protocol to download files to the switch.

LSD10524

First Found-in Version: S5500SI-CMW520-R1205

Condition: When configuring TACACS authentication mode for SSH users.

Description: SFTP users can access the switch without authentication.

LSD11771

First Found-in Version: S5500SI-CMW520-R1205

Condition: When VLAN configuration changes on Trunk/Hybrid ports.

Description: The switch will still send loopback-detection packets with vlan id in old configuration, but loopback-detection function work correctly.

LSD12767

First Found-in Version: S5500SI-CMW520-R1205

Condition: When displaying IPv6 routing-table in Quidview software.

Description: The Destination address and NextHop address in the routing-table entries are all wrong.

LSD12783

First Found-in Version: S5500SI-CMW520-R1205

Condition: When the switch enables 802.1x using pap/chap authentication mode.

Description: The self-service of iNode client software is malfunction.

LSD13004

First Found-in Version: S5500SI-CMW520-R1205

Condition: When user modifies a fixed username and password about MAC authentication if user is online.

Description: User later can not authentication successfully.

LSD13018

First Found-in Version: S5500SI-CMW520-R1205

Condition: When change the designated fixed account and password used for MAC authentication, and modify the offline-detect timer.

Description: The operation of cutting all connection will be failed and some connections always exist.

LSD13223

First Found-in Version: S5500SI-CMW520-R1205

Condition: When the switch enables 802.1x and client software enables the function of upload IP address.

Description: User can not be authorized via 802.1x.

LSD13239

First Found-in Version: S5500SI-CMW520-R1205

Condition: When the switch has learned some IPv6 neighbor on 10GE port.

Description: the IPv6 neighbor can not be displayed in Quidview software.

LSD13342

First Found-in Version: S5500SI-CMW520-R1205

Condition: When cutting user connection in CAMS server.

Description: NAS client in switch does not response the offline reason correctly, the offline reason displayed is "Nas Error".

Resolved Problems in S5500SI-CMW520-R1205P03

LSD15053

First Found-in Version: S5500SI-CMW520-R1205P02

Condition: display the information of cooperation logo

Description: The cooperation logo should modify 'Huawei-3com' to 'H3C.'

HWD05841

First Found-in Version: S5500SI-CMW520-R1205

Condition: display the information of one physical port .

Description: The port MAC always is '000f-e207-f2e0' that is reserve by H3C, but should be the Bridge Mac of this device.

Resolved Problems in S5500SI-CMW520-R1205P02

LSD09970

First Found-in Version: S5500SI-CMW520-R1205

Condition: Using Device Manager software.

Description: When doing "Performance Monitor" operation, it will be failed to create a non-"Default Event" alarm item, and relevant mib node returns error information.

LSD10312

First Found-in Version: S5500SI-CMW520-R1205

Condition: After the members are added to "Black List", disable cluster, and then enable cluster.

Description: The members are still in the "Black List".

LSD10325

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable MAC authentication.

Description: The MAC format of MAC authentication is "XXXXXXXXXXXX", and does not support format of "XX-XX-XX-XX-XX-XX".

LSD10349

First Found-in Version: S5500SI-CMW520-R1205

Condition: With terminal debugging enabled, execute pki request-certificate domain <name> command.

Description: If it fails to receive a certificate, the debugging information "Fail to retrieval CA certificate of the domain <name>" should be "Failed to receive a certificate from the ca domain <name>".

LSD10355

First Found-in Version: S5500SI-CMW520-R1205

Condition: Configuring the host name as the RSA public key.

Description: The configuration doesn't work.

LSD10359

First Found-in Version: S5500SI-CMW520-R1205

Condition: Using Device Manager software.

Description: Expansion module is displayed in front panel.

LSD10369

First Found-in Version: S5500SI-CMW520-R1205

Condition: Configuring wrong MIB object index in RMON alarm.

Description: The Get operation works, but the value is meaningless.

LSD10373

First Found-in Version: S5500SI-CMW520-R1205

Condition: Setting SNMP's RMON MIB node.

Description: The switch can not process too long OID variable correctly.

LSD10381

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable Multicast-vlan, and configure a link-aggregation port into a group of Multicast subvlans.

Description: It may cause multicast packet replication lost from subvlans.

LSD10388

First Found-in Version: S5500SI-CMW520-R1205

Condition: Do hot-swap of expansion module when system starting,

Description: The RMON statistics of expansion module port is wrong.

LSD10401

First Found-in Version: S5500SI-CMW520-R1205

Condition: Firstly enable loopback-detection for a trunk port; secondly change the trunk port's to the access type; thirdly disable loopback-detection; fourthly change the port's type to the trunk type.

Description: An unexpected configuration of "loopback-detection control enable" will be added in switch and can't be removed any more.

LSD10415

First Found-in Version: S5500SI-CMW520-R1205

Condition: Using the command of "command-privilege level 3 view shell debugging" in the system view, the command debugging has been configured as a higher privilege level command.

Description: Lower-level privilege users are still able to use the command.

LSD10548

First Found-in Version: S5500SI-CMW520-R1205

Condition: The default value of RIP's garbage-collect timer is 240 seconds.

Description: The value does not comply with the RFC description, should be 120 seconds.

LSD10591

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable RIP.

Description: The switch will advertise inactive routes.

LSD10593

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable MLD-snooping in VLAN, and configure host-join on a multicast group in a certain port.

Description: The host-join port can't join any MLD multicast group.

LSD10597

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable clustering.

Description: The switches can't telnet each other because telnet server in switch is disabled by default.

LSD10599

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable clustering.

Description: Wrong warning message issued from the Administrator unit when the command "cluster switch-to administrator" is issued. A more precise message would be "This is the administrator unit. Issue this command from a member unit."

LSD10680

First Found-in Version: S5500SI-CMW520-R1205

Condition: Setting the maximum mac number on a port, then display the maximum of mac number on the port using WEB interface.

Description: Result of the setting displayed on the web page is not correct. The maximum mac number is followed with a "%".

LSD10994

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable loopback-detection on ports in a link-aggregation, loopback-detection protocol packets will be sent from one port in the link-aggregation and other ports in the link-aggregation received the packet.

Description: Loopback-detection function will not work correctly.

LSD11077

First Found-in Version: S5500SI-CMW520-R1205

Condition: Setting a too long value to the MIB node etherStatsDataSource.

Description: The switch reboots.

LSD11764

First Found-in Version: S5500SI-CMW520-R1205

Condition: Enable STP.

Description: The switch does not process any STP Topology Changes (TCN) packets received.

LSD12291

First Found-in Version: S5500SI-CMW520-R1205

Condition: The link-aggregation includes more than two member ports.

Description: The switch CPU can not receive any packets from those ports.

Documentation

Related Documentation

Table 8 Related manuals

Manual	Version
H3C S5500-SI/EI Series Ethernet Switches Configuration Guides-Release 2208	6W100
H3C S5500-SI/EI Series Ethernet Switches Command References-Release 2208	6W100
H3C S5500-SI Complete Series Ethernet Switches Installation Guide	V1.02
H3C S5500-SI Complete Series Ethernet Switches Quick Start	V1.02
H3C S5500-SI Complete Series Ethernet Switches Compliance and Safety Manual	V1.04

Online Technical Support

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

Table 9 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	<p>Approach 1:</p> <p>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.</p> <p>Approach 2:</p> <p>In the homepage of H3C at http:// www.h3c.com, select Support > Technical Documents. Then select a product for its documents.</p>

Software Upgrading

CAUTION:

Upgrade software only when necessary and under the guidance of a technical support engineer.

This chapter introduces how to load BootROM and host software into a switch locally and how to do this remotely.

Introduction to Loading Modes

You can load the software locally by using:

- XModem via Console port
- TFTP via Ethernet port
- FTP via Ethernet port

You can load the software remotely by using:

- FTP
- TFTP

NOTE:

The BootROM software version must match the host software version when you load the BootROM and host software.

Local Software Loading

If your terminal is directly connected to the switch, you can load BootROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch to insure successful software loading.

NOTE:

The loading process of the BootROM software is the same as that of the host software, except that during the BootROM loading process, you must enter the different digit after entering the Boot Menu and the system gives somewhat different prompts. The following text mainly describes the BootROM loading process.

Boot Menu

Starting.....

```

*****
*
*          H3C S5500-28C-SI BOOTROM, Version 502          *
*
*****
Copyright (c) 2004-2009 Hangzhou H3C Tech. Co., Ltd.
Creation date   : Jun 19 2009, 15:19:51
CPU Clock Speed : 264MHz
BUS Clock Speed : 33MHz
Memory Size    : 128MB

```

Mac Address : 00e0fc005502

Press Ctrl-B to enter Boot Menu... 1

NOTE:

To enter the Boot Menu, you must press <Ctrl+B> within two seconds after the information "Press Ctrl-B to enter Boot Menu..." appears. Otherwise, the system starts to decompress the program; and if you want to enter the Boot Menu at this time, you will have to restart the switch.

Input the correct BootROM password (by default, no password is set on the switch). The system enters the Boot Menu:

BOOT MENU

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

Enter your choice(0-9):

Loading Software Using XModem Via Console Port

Introduction to XModem

XModem is a file transfer protocol that is widely used due to its simplicity and good performance. XModem transfers files via Console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and error packet retransmission mechanism (generally the maximum number of retransmission attempts is ten).

The XModem transmission procedure is completed by the cooperation of a receiving program and a sending program. The receiving program sends a negotiation packet to negotiate a packet check method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends an acknowledgement packet and the sending program proceeds to send another packet; otherwise, the receiving program sends a negative acknowledgement packet and the sending program retransmits the packet.

Loading BootROM software

Step 1: At the prompt "Enter your choice(0-9):" select 6 in the Boot Menu and then press <Enter> to enter the BootROM update menu shown below:

Bootrom update menu:

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):

Step 2: Enter 3 in the above menu to load the BootROM and host software using XModem protocol. The system displays the following download baud rate setting menu:

Please select your download baudrate:

- 1.* 9600
2. 19200
3. 38400
4. 57600
5. 115200
0. Return

Enter your choice (0-5):

Step 3: Choose an appropriate download baud rate. For example, if you enter 5, the 115200 bps rate is chosen, and the system displays 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

The fields above show that the baud rate has been changed, and now you can press <Enter>.

NOTE:

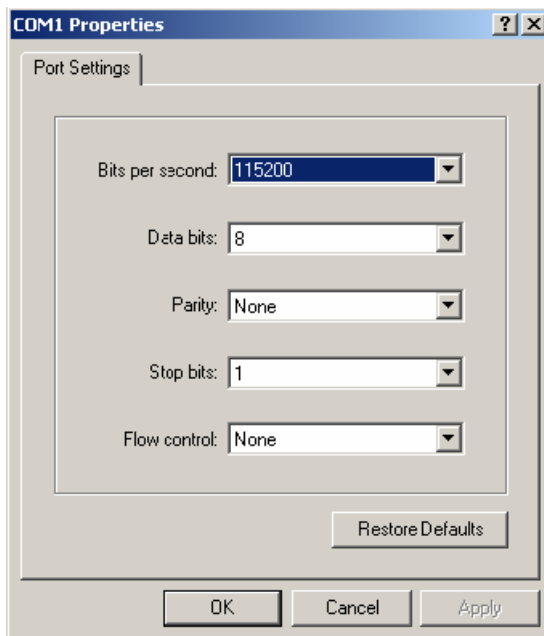
If you have chosen 9,600 bps, you do not need to modify the HyperTerminal's baud rate, and therefore you can skip Step 4 and 5 below and proceed to Step 6 directly. In this case, the system will not display the above information.

Step 4: Choose [File/Properties] in HyperTerminal, click <Configuration> in the popup dialog box, select the baud rate of 115,200 bps in the appeared Console port configuration dialog box.

Figure 1 Properties dialog box

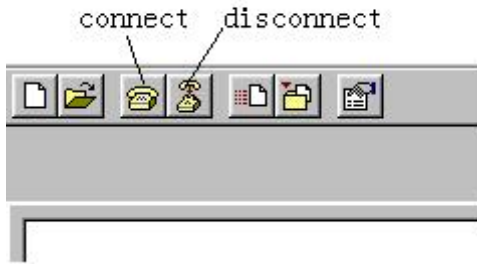


Figure 2 Console port configuration dialog box



Step 5: After setting the baud rate, you need to disconnect and the reconnect HyperTerminal so that the baud rate setting takes effect. Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch.

Figure 3 Connect and disconnect buttons



NOTE:

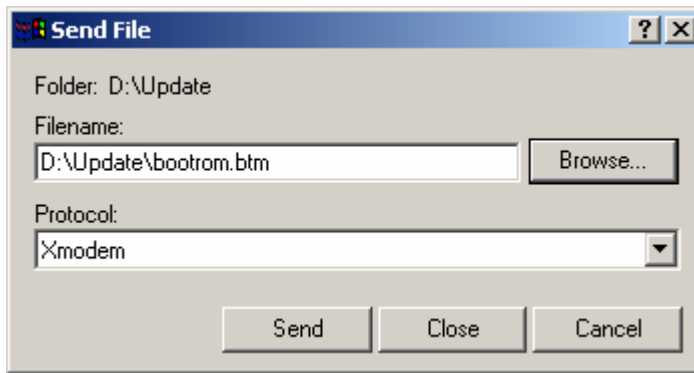
The new baud rate takes effect only after you disconnect and reconnect the terminal emulation program.

Step 6: Press <Enter> to start downloading the program. The system displays the following information:

```
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCCCC
```

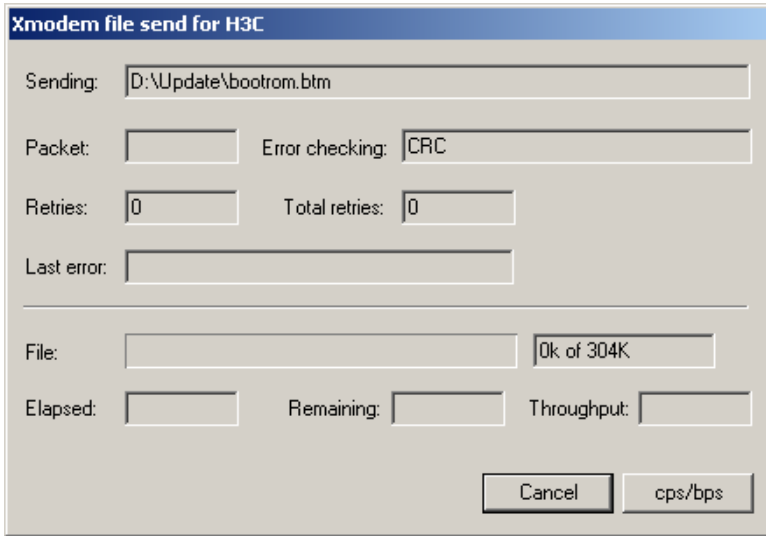
Step 7: Choose [Transfer/Send File] in the HyperTerminal's window, and in the following popup dialog box click <Browse>, select the software you need to download, and set the protocol to XModem.

Figure 4 Send file dialog box



Step 8: Click <Send>. The system displays the following page.

Figure 5 Page for file sending



Step 9: After the download completes, the system displays the following information:
Loading ...CCCCCCCC done!

NOTE:

You do not need to reset the HyperTerminal's baud rate and can skip the last step if you have chosen 9600 bps. In this case, the system displays the prompt "BootROM is updating now.....done!" instead of the prompt "Your baudrate should be set to 9600 bps again! Press enter key when ready".

Step 10: Reset HyperTerminal's baud rate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information to show the loading process is done.

Bootrom updating.....done!

Loading host software

Step 1: Select 1 in Boot Menu to load the host software of the switch. The system displays the following information:

- 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

To load the host software through XModem, select 3.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

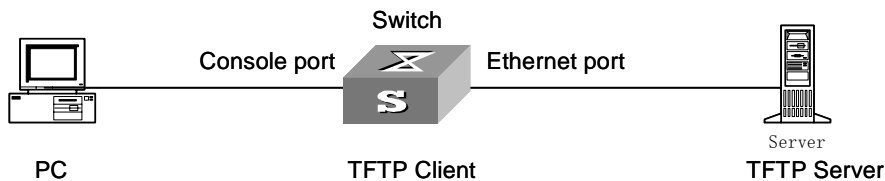
Loading Software Using TFTP Via Ethernet Port

Introduction to TFTP

Trivial file transfer protocol (TFTP), a protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It uses UDP to provide unreliable data stream transfer service.

Loading BootROM software

Figure 6 Load BootROM software via TFTP



Step 1: As shown in [Figure 6](#), connect the switch via an Ethernet port to the TFTP server, and connect the switch via the Console port to the configuration PC.

NOTE:

You can use one PC as both configuration device and TFTP server.

Step 2: Run the TFTP server program on the TFTP server, and specify the path of the program to be loaded.

CAUTION:

TFTP server program is not provided with the H3C Series Switches.

Step 3: Run the terminal emulation program on the configuration PC. Start the switch. Then enter the Boot Menu. At the prompt "Enter your choice(0-9):" select 6 in the Boot Menu and then press <Enter> to enter the BootROM update menu shown below:

Bootrom update menu:

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):

Step 4: Select 1 in the BootROM update menu to download the BootROM software using TFTP. Then set the following TFTP-related parameters as required:

```

Load File name      :S5500-SI.btm
Switch IP address   :1.1.1.2
Server IP address   :1.1.1.1
  
```

Step 5: Press <Enter> after inputting the information above. The system displays the following information:

```

Are you sure to update your bootrom?Yes or No(Y/N)
  
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the BootROM software. Upon completion, the system displays the following information to show the loading process is completed:

```
Loading.....done
Bootrom updating.....done!
```

Loading host software

Step 1: Select 1 in Boot Menu to load the host software of the switch. The system displays the following information:

```
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
```

To load the host software via XModem, select 1.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

Loading Software Using FTP Via Ethernet Port

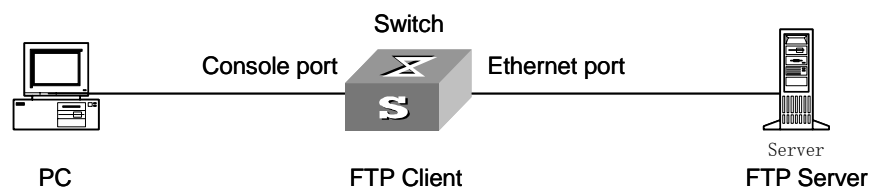
Introduction to FTP

File transfer protocol (FTP) is an application-layer protocol in the TCP/IP protocol suite. It is used for transferring files between server and client, and is widely used in IP networks.

You can use FTP to load software onto the switch via an Ethernet port. In this case, the switch can act as an FTP server or an FTP client. In the following example, the switch acts as an FTP client.

Loading BootROM software

Figure 7 Load BootROM software via FTP



Step 1: As shown in [Figure 7](#), connect the switch via an Ethernet port to the FTP server, and connect the switch via the Console port to the configuration PC.

NOTE:

You can use one PC as both configuration device and FTP server.

Step 2: Run the FTP server program on the FTP server, configure an FTP user name and password, and specify the path of the program to be downloaded.

Step 3: Run the terminal emulation program on the configuration PC. Start the switch. Then enter the Boot Menu.

At the prompt "Enter your choice(0-9):" select 6 in the Boot Menu, and then press <Enter> to enter the BootROM update menu shown below:

Bootrom update menu:

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):

Step 4: Enter 2 in the above menu to download the BootROM software using FTP. Then set the following FTP-related parameters as required:

```
Load File name       :S5500-SI.btm
Switch IP address    :10.1.1.2
Server IP address    :10.1.1.1
FTP User Name        :S5500
FTP User Password    :123
```

Step 5: Press <Enter> after inputting the information above. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the BootROM update menu. If you enter Y, the system begins to download and update the program. Upon completion, the system displays the following information:

```
Loading.....done
Bootrom updating.....done!
```

Loading host software

Step 1: Select 1 in Boot Menu to load the host software of the switch. The system displays the following information:

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

To load the host software via FTP, select 2.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

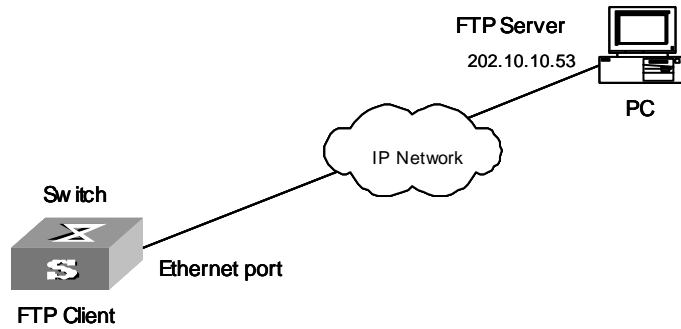
Remote Software Loading

You can telnet to the switch, and use FTP or TFTP to load BootROM and host software remotely.

Remote Loading Using FTP

As shown in [Figure 8](#), a PC is used as both configuration device and FTP server. You can telnet to the switch, and then execute the FTP commands to download the host program S5500-SI.bin and the BootROM program S5500-SI.btm from the remote FTP server (with IP address 202.10.10.53) to the switch.

Figure 8 Load software using FTP remotely



Step 1: Download the software to the switch using FTP commands.

```
<H3C> ftp 202.10.10.63
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):S5500
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get S5500-SI.bin
[ftp] get S5500-SI.btm
[ftp] bye
```

Step 2: Update the BootROM program on the switch.

```
<H3C> bootrom update file S5500-SI.btm slot 1
This command will update BootRom file, Continue? [Y/N]y
Updating BootRom, please wait...
```

Step 3: Update the host software on the switch.

```
<H3C> boot-loader file S5500-SI.bin slot all main
<H3C> display boot-loader
Slot 1
The current boot app is: flash:/ S5500-SI.bin
The main boot app is: flash:/ S5500-SI.bin
The backup boot app is: flash:/ S5500-SIbak.bin
```

Step 4: Restart the switch.

```
<H3C> reboot
```

NOTE:

Before restarting the switch, make sure other configurations are all saved to avoid the loss of configuration information.

After the steps above, the BootROM and host software loading is completed.

Pay attention to the following points:

- Host software loading takes effect only after you restart the switch with the reboot command.
- If the space of the flash memory is not enough, you can delete the useless files in the flash memory before software downloading.
- Power interruption is not allowed during software loading.

Remote Loading Using TFTP

The remote loading by using TFTP is similar to the remote loading by using FTP. The only difference is that it is TFTP that you use when loading software to the switch. In this case, the switch can only be used as a TFTP client.

Copyright © 2010 Hangzhou H3C Technologies Co., Ltd. All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Hangzhou H3C Technologies Co., Ltd.

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