Switch 5500 V3.03.02e Release Notes

Keywords: Resolved Problems, Software Upgrading

Abstract: *version information, updating, unresolved Problems and Avoidance Measures, List of Solved Problems.*

Acronyms:

Abbreviations	Full spelling
ACL	Access Control List
CLI	Command line interface
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GVRP	GARP VLAN Registration Protocol
HGMP	Huawei Group Management Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation control protocol
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
NDP	Neighbor Discovery Protocol
NTP	Net Time Protocol
QOS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SP	Strict Priority
SSH	Secure Shell

Abbreviations	Full spelling
STP	Spanning Tree Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
3ND	3Com Network Director

Table of Contents

List of Tables

Version Information

Version Number

Version Information: 3Com OS V3.03.02s56e

3Com OS V3.03.02s168e

Note: This version number can be displayed by command **display version** under any view. Please see **Note①**.

Version History

Table 1 Version history

Version number	Last version	Release Date	Remarks
V3.03.02s56e V3.03.02s168e	V3.03.01s56ep04 V3.03.01s168ep04	2008-10-31	New features version
V3.03.01s56ep04 V3.03.01s168ep04	V3.03.01s56ep03 V3.03.01s168ep03	2008-05-13	None
V3.03.01s56ep03 V3.03.01s168ep03	V3.03.01s56ep02 V3.03.01s168ep02	2008-03-20	None
V3.03.01s56ep02 V3.03.01s168ep02	V3.03.01s56ep01 V3.03.01s168ep01	2008-02-21	None
V3.03.01s56ep01 V3.03.01s168ep01	V3.03.00s56e V3.03.00s168e	2008-01-25	None
V3.03.00s56e V3.03.00s168e	None	2007-08-25	The first release of V3.03.xx.

Hardware and Software Compatibility Matrix

Table 2 Compatibility matrix

Item	Specifications
Product family	Switch 5500 Series Routing Switches

Item	Specifications
Hardware platform	5500-EI 28-Port (3CR17161-91) 5500-EI 52-Port (3CR17162-91) 5500-EI 28-Port PWR (3CR17171-91) 5500-EI 48-Port PWR (3CR17172-91) 5500-EI 28-Port FX (3CR17181-91) 5500-SI 28-Port(3CR17151-91) 5500-SI 52-Port(3CR17152-91)
Minimum memory requirements	64M
Minimum Flash requirements	16 MB
Boot ROM version	Version 3.03 (Note: This version number can be displayed by command **display version** under any view. Please see **Note②**)
Host software	s4m03_03_02s56e.app s4m03_03_02s168e.app
DM version	3Com DM V4.0 SP05 R0001
Web version	V4.00
Remarks	s4m03_03_02s56e.app is 5500 app 56-bit encryption for SSH s4m03_03_02s168e.app is 5500 app 168-bit encryption for SSH

Caution

V3.03.00 is the first release of V3.03.xx series. Some new features are added on the basis of V3.02.xx. Please refer to “Changed Features” for detail.

V3.02.xx and Bootrom V2.0x belong to one series of version, software enhancement project, which generally provides more software features and 3.01.xx and Bootrom V1.00 belong to another series.

Software version before V3.01.04 can be upgraded to later software version (V03.01.04 or later), for example, V3.01.02 can be upgraded to V3.01.04; while the later can not be downgraded to the former, for example, V3.01.04 can not be downgraded to V3.01.02.

To run older version application on switch with new version FLASH will generate following question:

Using FTP method to update application of these switches, or executing some commands such as "display diagnostic-information" which are relative to writing operation of Flash are executed on such switches, some errors will occur and command failed. Newer version (release number is 3.01.12p01 or later) has properly fixed the problem.

From V3.02.00p01, the new compressing arithmetic is applied and the size of APP is reduced.

Sample:To display the host software and bootrom version of the Switch 5500 Series Routing Switches, perform the following:

```
<5500-SI >disp ver
3Com Corporation
Switch 5500-EI Software Version 3Com OS V3.xx.xx              --- Note①
Copyright (c) 2004-2008 3Com Corporation and its licensors, All rights reserved.
Switch 5500-EI uptime is 0 week, 0 day, 0 hour, 1 minute

Switch 5500-EI 28-Port with 1 MIPS Processor
64M     bytes DRAM
16384K  bytes Flash Memory
Config Register points to FLASH

CPLD Version is CPLD 001
Bootrom Version is xxx                                        ---  Note②
[Subslot 0] 24 FE + 4 GE Hardware Version is 00.00.00
```

Restrictions and Cautions

Please use pps mode when doing storm suppression, because it is inaccurate in ratio mode.

Forwarding capacity of some ports can not reach the wire speed when the device is under the full-meshed test.

The system default anti-attack function may be affected if the queue-schedule is changed. Please leave queue-schedule unchanged if there is no special requirement .

Silicon behaviour: the IP packets with option field can not be forwarded .

Only support psftp client of a third-party software named putty when the device is used as SSH Server.

Giant frame:Packets with 1522 (including VLAN tag) length are counted for giant, and treated as error packets.

Notification of using outbound ACLs:

1. Packets sent out from CPU will not be mirrored, filtered, or prioritized.
2. Only the known unicast packets can be mirrored, filtered, or prioritized by outbound ACL, while the broadcast, multicast, and unknown unicast packets can not.
3. Outbound ACL (packet-filter outbound, mirrored-to outbound, traffic-priority outbound) will not work when the egress port is a member of a link-aggregation.

Limitation of port mirroring: The packets sent by CPU cannot be mirrored on egress port.

Do not use vlan-mapping with voice vlan , 802.1x, mac authentication, port-security, mac-max-count ,which is strongly suggested.

An inexistent destination VLAN could be configured in mac-address-mapping, and the corresponding MAC entry replication in the VLAN is actually done.

ARP Inspection, IP source guard features do not support link-aggregation ports.

DHCP snooping can't work together with QinQ.

When mac-address-mapping and link-aggregation are needed to work on the same port, please configure mac-address-mapping first, then configure link-aggregation; while when removing mac-address-mapping, please remove link-aggregation first. When there are lots of MAC addresses needed to be mapped, please do not do shutdown and undo shutdown operation frequently.

The destination MAC address for smartlink is 01-0f-e2-00-00-04.

Change to Notification of cooperation about stacking and dhcp-snooping trust

When configuring “dhcp-snooping trust” on a stack, and if the current running version is degraded from V3.03.01ep01or new version to old version before V3.03.01ep01, then “dhcp-snooping trust” should be configured on stack ports again and saved the configuration after rebooting, in this way the relative configuration of “dhcp-snooping trust” can work reliably.

Notice about NTP configuration in stacked devices

For stacked devices including NTP configuration, when upgrading the software from version between V3.03.00e and V3.03.01ep04 to V3.03.02e or newer version, the NTP configuration should be removed firstly then re-configured after stacking reboot.

Feature List

Hardware Features

Table 3 Hardware features

Category	Description
Size(Width×Height×Depth)	440mm×43.6mm×260mm(none PWR devices) 440mm×43.6mm×420mm(PWR devices)
Weight	≤3.5Kg(28 Port none PWR devices) ≤4Kg(52 Port none PWR devices)

Category	Description
	≤5.8Kg(28 Port PWR devices) ≤6.2Kg(52 Port PWR devices)
Input voltage	AC:Rated Voltage range:100-240V; 50/60Hz Max Voltage range:90-264V; 50/60Hz DC:Rated Voltage range:-60 - -48V Max Voltage range:-72 - -36V
System max power consumption	40W(28 Port none PWR devices) 50W(52 Port none PWR devices) 380W(28 Port PWR devices) 380W(52 Port PWR devices)
Temperature	0℃~45℃
Relative humidity	10%~90%

Software Features

Table 4 Software features

Features	Description
XRN	
Cluster	Cluster protocol, HGMP
RSTP/MSTP	Supporting STP, IEEE 802.1D/802.1s-compliant, standard MSTP
Flow control	IEEE 802.3x-compliant flow control for full-duplex Back-pressure based flow control for half-duplex
Port auto-negotiation	both speed and duplex mode auto-negotiation
MAC address table	Address learning Port binding-supported Table size: Up to 16K MAC addresses including 256 static mac addresses
Jumbo Frame	Jumbo frame support, up to 9 Kb per frame(only supported on 5500-EI)
QinQ	802.1Q in 802.1Q, double tag per port configuration
QinQ BPDU tunnel	bpdu packets can get through port which enable QinQ
POE/POE profile	Poe profile to configure poe parameters and mib is supported (only supported on 5500-EI)
Link aggregation	Up to 8 aggregation group, up to 8 FE ports or 4 GE per group Supporting link aggregation across unit

Features	Description
VLAN	Supporting port-based VLANs Up to 4K IEEE 802.1Q-compliant VLANs for 5500-EI and up to 256 VLANs for 5500-SI Bulk VLAN creation
GVRP	
Protocol based VLAN	802.1v, it supports IPV4 /IPX/AppleTalk(only supported on 5500-EI)
DLDP	Device Link Detection Protocol,single direction link status detection, private protocol
VCT	Virtual cable test
Port internal loop/external loop tests	The tests provide means to online detect port faults, the internal loop test is used to diagnose the physical channels between switch chips and PHY chips; the external loop test is used to diagnose the physical channels between PHY chips and network interfaces with the help of self-loop header. The two tests used together can distinguish whether a fault is a switch fault or a link fault.
Loopback detection	
Voice vlan	The voice VLAN feature is able to add ports into voice VLANs by identifying the source MAC addresses of packets. It automatically assigns priority rules, ensures that voice traffic takes appropriate priority so as to ensure the voice quality. This feature supports two application modes: manual and automatic. 5500 can work with cisco ip phone.
Unicast, multicast and broadcast packets suppression	Configured based on ports Supporting suppression by bandwidth ratio and suppression by pps (packets per second) broadcast suppression global configuration
802.1X authentication	The main purpose of the IEEE 802.1x protocol is to implement authentication for wireless LAN users. But its application in LANs defined by IEEE 802 LAN standards provides a method of authentication for LAN users.
Centralized MAC address authentication	Centralized MAC address authentication is triggered by users' data packets. In this authentication, users' MAC addresses are used as both user names and passwords. Upon receiving the first packet from a user, the switch retrieves the source MAC address from the packet, adds the address to both user name and password fields in a radius packet, and sends the radius packet (authentication packet) to a radius server. The remaining processing procedure is similar to 802.1x. If the password authentication on the server passes, the source MAC address is added to the MAC address table on the switch, and the user is permitted to access the network.
table full traps	when table is full, the trap will be sent for mac/arp /routing table
Guest VLAN	Before authentication or after authentication failure, it can access the resource of guest vlan Guest vlan for 802.1x
IP+MAC+PORT binding	
Port security	support multiple mode for port security
SSHv2	

Features	Description
TACACS+	Tacacs+ feature is improved based on the standard RFC1492, it can implement multiple AAA authentication via Server-Client mode. This function is more security than Radius. only support single unit
Password control	Password control feature is focused on the password ageing management. When a user enters a switch, the switch will tell him how many days the password will be expired. If the password is not expired the switch will says the remainder days and allow user to modify the password. When the user sets the new password, the switch will record the new code and creation time and date. If the user does not modify the password he can use the old password to access the switch; When the password is expired, the switch will inform user about this case and a new password must be entered and confirmed. If the password is illegal and the twice confirmations fail, the user must re-enter the password.
AM	
ARP	Also support gratuitous arp
Multicast	IGMP(Internet Group Management Protocol) PIM-DM(Protocol Independent Multicast-Dense Mode) PIM-SM(Protocol Independent Multicast-Sparse Mode) (only supported on 5500-EI)
IGMP group policy	support IGMP group limit/ policy to filter unnecessary IGMP packets via software (only supported on 5500-EI)
IGMP snooping group policy	Support IGSP group policy to filter unnecessary IGMP packets via software
IGMP snooping querier	IGSP querier in layer2 mode
multicast source check	support the multicast source check to protect illegal multicast intrusion
MVR	multicast VLAN register, this feature will reduce the multicast traffic duplication. All nodes share one copy of multicast traffic with igmp snooping protocol.
MSDP	multicast source discovery protocol, only support single unit(only supported on 5500-EI)
Static multicast address configuration by manual	Allow to configure static multicast address to include some ports
Unknown multicast drop	
IGMP proxy	(only supported on 5500-EI)
IGMP SNOOPING	IGMP Snooping (Internet group management protocol snooping) is a multicast control mechanism operating on Layer 2 Ethernet switches, which is used to manage and control multicast groups.
VRRP	(only supported on 5500-EI)
DHCP server	embedded dhcp serve(only supported on 5500-EI)

Features	Description
Dhcp-relay	The earlier DHCP protocol only applies to the circumstances that DHCP clients and DHCP servers are in the same subnet and cannot operate across network segments. Therefore, to implement dynamic host address assignment, each subnet should be deployed with a DHCP server. This is obviously uneconomical. DHCP Relay is introduced to resolve this problem. Through a DHCP relay, DHCP clients in a LAN can communicate with a DHCP server in another subnet to obtain valid IP addresses. In this way, DHCP clients in multiple networks can share one DHCP server. This saves costs and helps to implement centralized management.
DHCP snooping	snoop dhcp packets in layer2 mode
Fake dhcp server detection	Fake dhcp server detection in dhcp relay
IP routing	Static routes RIP(Routing Information Protocol) RIP support ECMP OSPF(only supported on 5500-EI)
NTP	Along with the ever growing of network complicity, clock synchronization between the devices in a network becomes more and more important. NTP (network time protocol), a protocol built on top of TCP/IP, is used to distribute accurate time in a network.
QoS	Bandwidth management Priority setting based on VLAN port, IEEE 801.1P, ToS/Diffserv, and CoS 8 sending queues per port Queue scheduling algorithms such as WFQ, SP, and WRR Traffic classification QoS profile
port mirroring	Including remote port mirroring and local mirroring For 5500-EI support both mode mirroring and 5500-SI only support local port mirroring. The remote port mirroring supports mirroring from a port to anywhere via vlan channel.
Software update	Software load and update through the XMODEM protocol Software load and update through FTP (file transfer protocol) and TFTP (trivial file transfer protocol) Supporting FTP/TFTP client, FTP server
FTP, TFTP, FTP SERVER	
ftp disconnect	Disconnect ftp link by command

Features	Description
System configuration and management	Configuration through CLI (command line interface) Configuration through the Console port Local/remote configuration through Telnet Remote configuration through Modem SNMP (simple network management protocol) based network management RMON (remote monitoring) 1/2/3/9 group MIBs System logging Hierarchical alarming
password recovery	Password recovery technique is adopted for the recovery of Boot ROM and APP passwords
Network maintenance	Filter, output, and statistics of alarm/debug information Diagnostic tools: Ping, Trace, and so on. Remote maintenance by Telnet and other ways
web	
Diagnostics and alarm output	When a switch operates, hardware/software problems may occur; quickly recording and reporting problems is important for troubleshooting the problems.
Fast startup	Both fast and normal start settings are supported. In fast start mode, the switch can start up within 60 seconds. This greatly increases the startup speed in comparison with previous switches When starting in fast mode, the switch skips the POST (power-on self-test) and runs the APP application directly. When starting in normal mode, the switch performs the whole POST. You can set the start mode to fast or normal by using the Boot ROM menu.

Version Updates

Feature Updates

Table 5 Feature updates

Version Number	Item	Description
V3.03.02e	Hardware feature updates	None
	Software feature updates	New Features: 1) SSHv1

Version Number	Item	Description
		2) Hot Patch 3) LLDP Deleted Features: IPv6 Please refer to the Operation Manual and Command Manual.
V3.03.01ep04	Hardware feature updates	None
	Software feature updates	New Features: 1) IGMP protocol packet transparent 2) Local ARP proxy and ARP Proxy separate 3) RSA,DSA negotiation order can be self-select 4) Configure Prune Delay function
V3.03.01ep03	Hardware feature updates	None
	Software feature updates	New Features: Support RFC4188 and RFC2674.
V3.03.01ep02	Hardware feature updates	None
	Software feature updates	None
V3.03.01ep01	Hardware feature updates	None
	Software feature updates	New features: ARP source MAC consistency detection feature The feature can judge a packet whether it is spurious by checking both the source MAC in ether header and the source MAC in ARP header are uniform. If they are not uniform, the switch will not refresh the ARP entry.
V3.03.00e	Hardware feature updates	None
	Software feature updates	The following features are added to V3.03.00e on the basis of V3.02.xx. 1) DHCP Snooping security 2) Arp proxy and local arp proxy 3) VLAN mapping 4) Selective QINQ 5) VLAN ACL 6) IGMP snooping nonflooding

Version Number	Item	Description
		7) FTP banner 8) HTTP banner 9) Telnet copyright 10) Speed auto configuration 11) Port link delay 12) Configuring a Host Statically to Join a Group 13) Smartlink 14) BPDU TUNNEL enhancement 15) Designating router port manually 16) Storm constrain 17) Link type ACL (acl number 4000) supports inner VLAN range configuration, the inner VLAN range configuration with QACL action provide Selective QinQ for users. 18) Traffic-redirect action can redirect the packets as untagged, the default is tagged. Also supports redirect packets to master port in a link-aggregation group. 19) IPv6 management 20) DHCP snooping process dhcp nak and decline packets. 21) Enhanced SFP supported 22) Do local authentication when hwtacacs authentication fails 23) XRN auto stack 24) Port isolate across stack 25) EAP authentication mode for telnet user 26) Port security and or mode 27) Work with Cisco OSPF p2mp non-broadcast interface 28) RIP support offset modification 29) Cipher copy past for SNMP module 30) IGMPv3 Snooping 31) Long user name 32) SNMP mib-view mask configuration 33) MAC-authentication supports guest VLAN 34) Remote-ping test enhancement 35) DLDP recover 36) DHCP option 82 string

Version Number	Item	Description
		37) Super authentication for HWTACACS 38) HGMP topology management and trace MAC 39) EAD quickly employ 40) Web authentication 41) Web-based cluster 42) Implement some OSPF NSSA changes documented in RFC3101

Command Line Updates

Table 6 Command line updates

Version Number	Item	Description
V3.03.02e	New Commands	Please refer to the Operation Manual and Command Manual.
	Deleted Commands	Please refer to the Operation Manual and Command Manual.
	Modified Commands	Please refer to the Operation Manual and Command Manual.
V3.03.01ep04	New Commands	Command 1: Syntax: [undo] igmp transparent enable View: Ethernet interface view Description: This command enables/disables igmp transparent function. Example: [Switch-Ethernet1/0/4] igmp transparent enable Command 2: Syntax: [undo] local-proxy-arp enable View: vlan interface view Description: This command enables/disables local-proxy-arp function. Example: <Switch> system-view [Switch] interface Vlan-interface 3 [Switch-Vlan-interface3] local-proxy-arp enable Command 3:

Version Number	Item	Description
		Syntax: [undo] prune delay interval View: PIM view Description: This command sets the interval of prune delay. Example: < Switch > system-view System View: return to User View with Ctrl+Z. [Switch] multicast routing-enable [Switch] pim [Switch -pim] prune delay 75
	Removed commands	None
	Modified Commands	None
V3.03.01ep03	New Commands	None
	Removed commands	None
	Modified Commands	None
V3.03.01ep02	New Commands	None
	Removed commands	None
	Modified Commands	None
V3.03.01ep01	New Commands	Command 1: Syntax: [undo] loopback-detection shutdown enable View: interface view Description: This command enables/disables loopback-detection shutdown function. Example: [Switch-Ethernet1/0/4]loopback-detection shutdown enable Command 2: Syntax: [undo] arp anti-attack valid-check enable View: system view Description: This command enables/disables “ARP source MAC consistency detection” function. Example: [Switch] arp anti-attack valid-check enable
	Removed commands	None
	Modified Commands	None
V3.03.00e	New Commands	Please refer to the documents provided by 3Com.

Version Number	Item	Description
	Removed commands	Command 1: Syntax: multicast load-sharing enable {global-hash | local-hash} undo multicast load-sharing enable Reason: The link-aggregation supports multicast load-sharing by default. It the same as unicast forwarding. Command 2: Syntax : display workpath Reason: This is a debugging command. Command 3: Syntax: spt-switch-threshold INTEGER<0-65535> [group-policy INTEGER<0-4294967295> [order INTEGER<1-99>]] View: PIM view Reason: The switch chip does not support multicast speed calculation. Command 4: Syntax: language-mode { english | chinese } View: user view Reason: do not support Chinese language mode.
	Modified Commands	Command 1: Syntax: rule [rule-id] { permit | deny } [[type protocol-type type-mask | lsap lsap-type type-mask] | format-type | cos cos | source { source-vlan-id | source-mac-addr source-mac-mask }* | dest { dest-mac-addr dest-mac-mask } | ***c-tag-vlan c-tag-vlan-begin [to c-tag-vlan-end]*** | time-range name]* undo rule rule-id View: acl 4000 view Parameters: c-tag-vlan c-tag-vlan-begin [to c-tag-vlan-end] defines the inner vlan range. Description: defines the inner VLAN range in port QINQ status which provide selective QINQ function for users.

Version Number	Item	Description
		Command 2: Syntax: traffic-redirect { inbound | outbound } *acl-rule* { cpu | { interface { *interface-name* | *interface-type interface-number* } | ***link-aggregation-group agg-id } [untagged]*** } undo traffic-redirect { inbound | outbound } *acl-rule* View: Ethernet interface view Parameters: link-aggregation-group agg-id : the link-aggregation group id for packets redirected to, the range is 1~416. Untagged: the default format the redirected packets is VLAN tagged. The user can configure the packets redirected as VLAN untagged. Command 3: Syntax: traffic-limit inbound { user-group *acl-number* [rule *rule*] | ip-group *acl-number* [rule *rule*] | link-group *acl-number* [rule *rule*] | user-group *acl-number* [rule *rule*] } ***[union-effect] [egress-port port]*** target-rate ***[burst-bucket burst_bucket_size]*** [exceed *action*] undo traffic-limit inbound { user-group *acl-number* [rule *rule*] | ip-group *acl-number* [rule *rule*] | link-group *acl-number* [rule *rule*] | user-group *acl-number* [rule *rule*] } Description: [union-effect]: the action includes permit or not, if there is no [union-effect], the traffic-limit will includes permit action for in-profile packets, otherwise not. [egress-port *port*]: traffic-limit can be apply to ingress port and egress port simultaneously. [burst-bucket *burst_bucket_size*]: the bucket size for burst traffic. The unit is kbytes Command 4: line-rate { inbound | outbound } target-rate ***[burst-bucket burst_bucket_size]*** Description: [burst-bucket *burst_bucket_size*] is same as traffic-limit. Command 5: display vlan , display vlan static, display vlan dynamic Description: diplay total VLAN number

Version Number	Item	Description
		[Switch]dis vlan Total 1547 VLAN exist(s). Now, the following VLAN exist(s): 1(default), 2-10, 100, 200, 512-1535, 2000, 3585-4094 [Switch]dis vlan sta Total 523 static VLAN exist(s). Now, the following static VLAN exist(s): 1(default), 2, 4-10, 100, 200, 512-1023 [Switch]dis vlan dy Total 1024 dynamic VLAN exist(s). Now, the following dynamic VLAN exist(s): 3, 1024-1535, 2000, 3585-4094 Command 6: VRRP related reset vrrp statistics ***interface*** STRING<1-256> STRING<1-256> [***vrid*** INTEGER<1-255>] reset vrrp statistics ***interface*** STRING<1-256> [***vrid*** INTEGER<1-255>] vrrp vrid INTEGER<1-255> track ***[interface]*** STRING<1-256> STRING<1-256> [reduced INTEGER<1-255>] vrrp vrid INTEGER<1-255> track ***[interface]*** STRING<1-256> [reduced INTEGER<1-255>] vrrp ***[vrid INTEGER<1-255>]*** authentication-mode { { simple STRING<1-8> } | { md5 STRING<1-256> } } Command 7: display ntdp [device-list [verbose] | single-device mac-address H-H-H] Description: display by single device

MIB Updates

None

Configuration Changes

Configuration Changes in V3.03.02e

1) Igmp-snooping nonflooding-enable and stack aren't mutualy exclusive any longer.
2) Change to the format of CDP packet.

A device sends CDP packets if voice vlan legacy is enabled. From current release, there is native VLAN information in the packet sent by device. The value of native VLAN is the pvid of the port. In early release, the packets sent by device don't contain native VLAN information.

3) Change to "Skip current configuration file" function in bootrom menu

In early release, a configuration file is always skipped if it is configured to skip in bootrom menu. In current release, the skip configuration takes effect only once.

4) Change to PAUSE-frame-sending

In the latest release, new command is provided to forbid sending PAUSE frame.

5) HWTACACS and stack aren't mutually exclusive any longer.
6) Change to voice VLAN function

In early release, the priority of the packets in voice VLAN is changed by default. The CoS is changed to 6, and the DSCP is change to 46.

In the latest release, the packets in voice VLAN are also changed by default as early release. However, several commands are provided to tune the priority-remarking action.

7) ARP inspection and stack aren't mutually exclusive any longer.
8) IP source guard and stack aren't mutually exclusive any longer.
9) Port-security port-mode auto-learn and stack aren't mutually exclusive any longer.
10) The performance of EAD is optimized.

Configuration Changes in V3.03.01ep03

1) Modification about dot1x timer tx-period command

Before Modification:

The range of 802.1x multicast request packet transfer period set by dot1x timer tx-period command is 10-120 seconds. Based on the rule that port will enter guest VLAN when 1 such packet get no response, the shortest time for entering guest VLAN is about 10 seconds.

After Modification:

The range of 802.1x multicast request packet transfer period set by dot1x timer tx-period command is 1-120 seconds. Based on the rule that port will enter guest VLAN when 1 such packet get no response, the shortest time for entering guest VLAN is about 1 seconds.

Configuration Changes in V3.03.01ep01

1) Change to loopback-detection function

A new choice "shutdown" is added to loopback-detection function. If loopback-detection shutdown is enabled and there is a loop under a port, the port will be shutdown. User can restore the port to UP state with command "undo shutdown". If a port is shutdown by loopback-detection, command "display interface" indicates the port is in "LOOPBACK-DETECTION DOWN" state, and "display brief interface" shows that the port is in "LPD DOWN" state.

Notes:

a) Loopback-detection shutdown is different from command line "shutdown" in some degree. If a port is shutdown by loopback-detection function, user can't see command "shutdown" by running "display this" under that port.

b) Loopback-detection shutdown function is mutually exclusive with loopback-detection control function.

2) Change to 802.1x function

In early version:

a) The 802.1x client passes the authentication. If the client changes its IP address, the switch will make the client log off.

b) The 802.1x client passes the authentication. If the client changes its IP address by using DHCP and the switch does not enable DHCP-Snooping function, the switch will make the client log off.

c) The 802.1x client passes the authentication. If the client changes its IP address by using DHCP and the switch enable DHCP-Snooping function, the switch will not make the client log off.

In current version:

The switch will not make the client log off when all the above mentioned three situations occur.

Configuration Changes in V3.03.00e

1) Info-center buildrun on the last configuration
2) Canceling the restriction for vlan-vpn coexisting with other protocols such as STP/GVRP.
3) The device as a tftp client can compatible with "\r\n" and"\n" wrap prompt, so we can upload or download files correctly with tftp server on UNIX system
4) Optimizing the ping performance, so the counter statistics are affected. The counter statistics is not as real-time as old version
5) The user can configure port mirror function by web
6) The device will forward the unknow 1x EAP type packets
7) The default DLDP interval time is changed to 5s, and the range is 1s~100s, in the previous versions, the interval time is 10s, and the range is 5s~100s. the DLDP cannot work with different interval time, user should modify the interval time to the same value.
8) The DLDP protocol number changed from 0800 to 8809, when V3.03.00e or later version work with V3.02.03 or earlier version, when the DLDP port stp status is discarding, the DLDP cannot function normally.
9) The matching sequence for web file is changed to default, main, backup, while before the sequence is main, backup, default.
10) Do not send PortMstiStateDiscarding trap and log when port status changed from up to down.

Open Problems and Workarounds

OLSD27415

- First Found-in Version: V3.02.00
- Description: In fabric system, after rebooting switch with saved configuration, undo ndp enable may be lost.
- Avoidance: None

OLSD26983

- First Found-in Version: V3.02.00

- Description: It may be occurring with little probability when many users login in with MAC-authentication, the connection number is zero, but the access number is nonzero, and the user cannot be deleted
- Avoidance: None

OLSD28340

- First Found-in Version: V3.02.00
- Description: the XRN stacked device which is designated as administrator cluster switch links with the member switch by slave device, if the member switch is under PASSIVE ftp mode, the ftp cluster will fail on getting packets.
- Avoidance: Change the cluster member switch ftp mode to PORT mode.Linking with the member switch by XRN master device.

LSOD02394

- First Found-in Version: V3.03.01ep01
- Description: Fabric system in cluster ping the partner with long frame from the slave unit maybe timeout with little probability.
- Avoidance: None

LSOD02873

- First Found-in Version: V3.03.01ep01
- Description: Enable link-aggregation accross unit and STP on a fabric system, and inject heavy traffic into link-aggregation ports. Change the physical link state of fabric ports frequently for a long time, it may cause the stack system break.
- Avoidance: None.

List of Resolved Problems

Resolved Problems in V3.03.02e

LSOD08196

- First Found-in Version: V3.03.01ep04
- Condition: Equipment as first-hop router, other manufacturers' equipment (for instance IP 8800 of NEC) as RP. RP can not create multicast forwarding table by PIM null-register packets. Multicast forwarding table of RP will be aged out when the link between the first-hop router and RP is interrupted.
- Description: The RP can not create multicast forwarding table after the interrupted link is recovered.

LSOD08193

- First Found-in Version: V3.03.01ep04
- Condition: Configure password information.
- Description: The password can be found in logbuffer, this is a hidden danger.

LSOD08145

- First Found-in Version: V3.03.01ep04
- Condition: Enable selective QinQ, and then configure a lot of mapping between outer tag and inner tag until the resource is exhausted.
- Description: The mapping between outer tag and inner tag can not be deleted. Only to restart the device can recover the problem.

Resolved Problems in V3.03.01ep04

LSOD07316

- First Found-in Version: V3.03.01e
- Condition: Do the 802.1x authentication with CAMS server. Before authentication the port's PVID is V1, the authorization VLAN ID assigned by the authentication is V2.
- Description: CAMS shows that he user's VLAN ID is V1, but not authorization VLAN(V2).

LSOD07416/LSOD07422/LSOD07420/LSOD01108

- First Found-in Version: V3.02.03
- Condition: For an 802.1x authentication port, the dynamical assigned VLAN id and previous PVID is not in the same MSTP instance.
- Description: Authentication fails.

LSOD07375

- First Found-in Version: V3.03.01e
- Condition: Send UDP packets whose destination port is 1645 or 1646 to the device.
- Description: Each UDP packet will cause switch lose 32 bytes memory.

LSOD07479

- First Found-in Version: V3.03.01ep02
- Condition: To disable and then enable device's STP periodically, and the network topology changed frequently.
- Description:The device may reboot without exception information.

LSOD07124

- First Found-in Version: V3.03.01ep02
- Condition: Stack serve as DHCP RELAY, PC gets IP address through it. And PC needs to send DHCP INFORM packet to get extra information after it got IP address successfully.
- Description: DHCP RELAY will not process DHCP ACK packet replied from DHCP server, which leads to PC can not process the DHCP ACK packet

LSOD07386

- First Found-in Version: V3.03.01ep01
- Condition: A loop is detected under a port after loopback-detection shutdown is enabled on that port.
- Description: An exception maybe occurs on the device.

LSOD07313

- First Found-in Version: V3.03.01e
- Condition: Exchange SFP modules on the same port in 5 seconds.
- Description: Check the SFP information with the command of display transceiver, the information is not updated.

LSOD07467

- First Found-in Version: V3.03.01ep02
- Condition: The egress traffic speed is higher than the speed of port A.
- Description: The dropped packets are not counted

LSOD07402

- First Found-in Version: V3.03.01ep02
- Condition: STP protocol is disabled globally or partly on some ports, and STP packets should be forwarded transparently.
- Description: STP packets are forwarded without any VLAN tag, that is, these packets have not filled the VLAN tag according to VLAN attributes of egress ports.

LSOD06140

- First Found-in Version: V3.03.01ep02
- Condition: Configure command "mac-address max-mac-count xxx" on one port, and then delete the learned dynamic mac addresses with command "undo mac-address".
- Description: The device can not learn new dynamic MAC address within 30 seconds.

LSOD06692

- First Found-in Version: V3.03.01ep02
- Condition: Enable OSPF feature in switch, and then set up OSPF neighbors. Attack the switch with packets whose destination IP is unknown on the switch.
- Description: The OSPF peers lost.

LSOD07412

- First Found-in Version: V3.03.01ep02
- Condition: Reboot the switch with its FE port inserted with one SFP module
- Description: The SFP module will be recognized as 100_SFP_UNKNOWN_CONNECTOR after the switch reboots.

LSOD07444

- First Found-in Version: V3.03.01ep02
- Condition: The type of SFP is 3CSFP85 or 3CSFP86
- Description: The device can not recognize that SFP.

Resolved Problems in V3.03.01ep03

LSOD07038

- First Found-in Version: V3.03.01ep02

- Condition: The stack serves as DHCP Relay, PC request IP address through DHCP Relay. After getting IP address, PC send inform packet to DHCP server.
- Description: When PC request IP address again, PC must repeat the request operation before it get IP address successfully.

LSOD07240

- First Found-in Version: V3.03.01ep02
- Condition: Send DHCP request packet to switch continued and reset DHCP relay security entry at the same time.
- Description: Switch is worked abnormal, reboot or can not build request temporary entry.

LSOD07138

- First Found-in Version: V3.03.01ep02
- Condition: Stack serve as DHCP snooping, PC request IP address through DHCP snooping.
- Description: Display DHCP snooping entry by display dhcp-snooping unit X command on unit X, the value of remaining lease always is 0.

LSOD07145

- First Found-in Version: V3.03.01ep02
- Condition: Administrative user do RADIUS authentication. The server simultaneously assign 2 types of attribute for administrative privilege, (Vendorid=43, Type=1) and (Vendorid=2011, Type=29).
- Description: RADIUS authentication fails.

LSOD07184

- First Found-in Version: V3.03.01ep02
- Condition: Stack joins in a cluster as a cluster member.
- Description: On slave, memory leaks 512 bytes per minute.

LSOD07234

- First Found-in Version: V3.03.01ep02
- Condition: Execute undo cluster enable command on stack device which works as a cluster member.
- Description: The cluster configuration of master device can not synchronize to salve device.

LSOD07128

- First Found-in Version: V3.03.01ep02
- Condition: For a stacking, STP bpdu-protection is configured on the device. STP edged-port on slave unit became 'Administrator Down' because of receiving BPDU.
- Description: Using command display stp portdown, the port with 'Administrator Down' state on slave can't be seen.

LSOD07143

- First Found-in Version: V3.03.01ep02

- Condition: Port A connecting to an end station is running STP and is not a STP edged-port, link status of this port changes from down to up.
- Description: STP status of port A in MSTI will change from discarding to forwarding directly, not passing learning state.

LSOD07136

- First Found-in Version: V3.03.01ep02
- Condition: Login in the device through telnet, when there is lots of IUC traffic.
- Description: The telnet user is hung up and the resource can not be freed.

LSOD07140

- First Found-in Version: V3.03.01ep02
- Condition: Two devices in stack, telnet users log in slave device. Use the free user-interface vty command to free telnet users on slave's console. Use the display users-interface command to view the user information on master device.
- Description: The master device reboots abnormally.

LSOD07162

- First Found-in Version: V3.03.01ep02
- Condition: On access port, execute loopback-detection shutdown enable command firstly and then execute loopback-detection enable command secondly.
- Description: The loopback-detection shutdown enable command invalid.

LSOD06680/LSOD07269

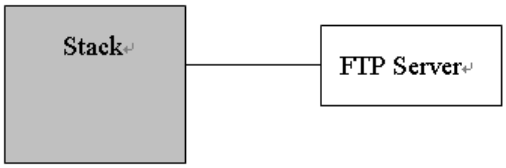
- First Found-in Version: V3.03.01ep02
- Condition: There is a default configuration file 'config.def ' on device. But not specify the startup saved-configuration.
- Description: Device does not use the autoconfig function to reboot, but use the 'config.def ' file to reboot.

ZDD01517

- First Found-in Version: V3.03.01ep02
- Condition: Use the network management tool of the AT&T Company to backup the configuration on device.
- Description: Memory will leak 512K bytes every time.

LSOD06530

- First Found-in Version: V3.03.01ep02
- Condition: The networking diagram is shown below: Stack as FTP client, FTP client and server are the same device of Switch S5500 series. Device A connects the FTP server indirectly.



- Description: Execute ftp put operation failed on device A.

LSOD06973

- First Found-in Version: V3.03.01ep02
- Condition: Enable ARP rate-limit on Port A and the input many ARP packets into it. The port A is shut down for ARP rate-limit. Do the operation of undo shutdown immediately on port A.
- Description: The operation of undo shutdown fails. Port A is still down all the time.

LSOD07239

- First Found-in Version: V3.03.01ep02
- Condition: The unit id of device is not 1. Enable DHCP rate-limite on port A and then enable DHCP-snooping.
- Description: The PC connecting to port A can not get IP dynamically

LSOD07214

- First Found-in Version: V3.03.01ep02
- Condition: Manage the POE device by WEB.
- Description: The WEB page can not be opened normally.

LSOD06010

- First Found-in Version: V3.03.01ep02
- Condition: Configure a static route marked with blackhole on the device, whose next hop address is a reachable valid IP address, such as 'ip route-static 1.1.1.0 255.255.255.0 2.2.2.2 blackhole'.
- Description: All the ip packets matching the blackhole route are still forwarded normally.

Resolved Problems in V3.03.01ep02

LSOD07030

- First Found-in Version: V3.03.01ep01
- Condition: Configure "dhcp-snooping trust" in every unit of stack, and save configuration, then reboot.
- Description: This command failed to be synchronized in stack, and this leads to the failed forwarding of dhcp packets.

LSOD07040

- First Found-in Version: V3.03.01ep01
- Condition: Port A is an FE fiber-optic port. The device rebooted after an FE fiber-optic module was inserted into port A.
- Description: Port A was recognized as a GE port.

LSOD06979

- First Found-in Version: V3.03.01ep01
- Condition: Under stack environment, a port of some UNIT detected TC or received TC BPDU.
- Description: The ARPs on ports of other UNIT can't be deleted.

LSOD06977

- First Found-in Version: V3.03.01ep01
- Condition: Under stack environment, some trunk consists of ports on different UNITs. System memory used rate is very high (e.g. free memory is lower than 2M).
- Description: Exception may occur on MSTP task, and the device will reboot itself.

LSOD06983

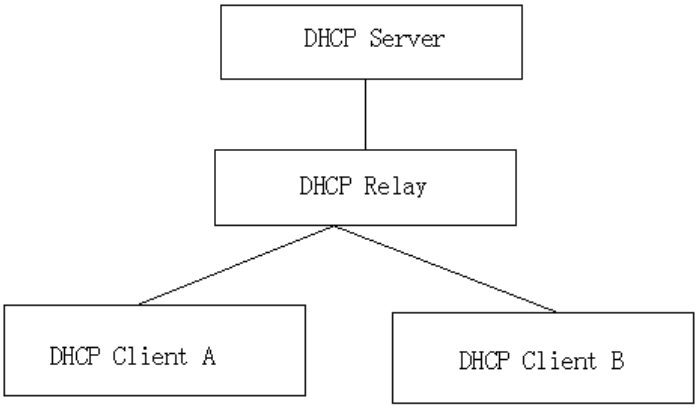
- First Found-in Version: V3.03.01ep01
- Condition: Enable DHCP snooping on stack, and the startup time of every unit is different on stack. DHCP client create dhcp-snooping item on stack.
- Description: Display DHCP snooping table, the lease of DHCP snooping item is different on different unit.

LSOD06999

- First Found-in Version: V3.03.01ep01
- Condition: Enable DHCP snooping trust on fabric port on stack, and upgrade from version A to version B, and then reboot stack.
- Description: Fabric port can not enable.
- Notes: version A supports DHCP snooping trust; version B can not support DHCP snooping trust.

LSOD07046

- First Found-in Version: V3.03.01ep01
- Condition:



- The figure is as above.
- DHCP Client A and B separately connect to the DHCP server to obtain IP address through DHCP relay. Client A has successfully obtained IP address IP_A, and then released the IP_A. Client B obtained the IP address with client-id information, and the DHCP server allocated IP_A to client B again.
- Description: After every operation, memory leaks 32 bytes.

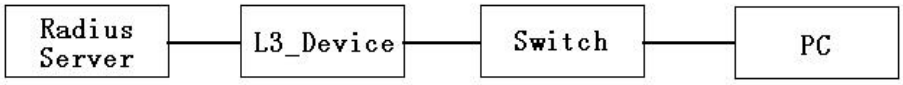
LSOD06981

- First Found-in Version: V3.03.01ep01
- Condition: Receive LACP protocol packet that not conform to the Protocol stipulated (124 bytes)

- Description: LACP protocol Packets are discarded because packets' length check failed, and so bring on aggregate fail.

LSOD06978

- First Found-in Version: V3.03.01ep01
- Condition: In the following network, enable EAD quick solution on the switch with only layer-2 forwarding who connects to authentication server via layer-3 device.



- Description: EAD quick solution can not bring into effect.

LSOD07065

- First found-in version: V3.03.01ep01
- Condition: Enable DHCP relay on switch, input DHCP request/ ACK packets continually. Execute display dhcp-security command.
- Description: The switch reboots abnormally.

Resolved Problems in V3.03.01ep01

LSOD05600

- First Found-in Version: V3.03.00e
- Condition: Enable "arp restricted-forwarding" on a stack, and the DHCP client and the DHCP server are connected to different units.
- Description: The client can not ping the server after the client gets ip address.

LSOD05954

- First Found-in Version: V3.03.00e
- Condition: Enable "dhcp-snooping" on a stack, and the master port of the uplink link-aggregation is down.
- Description: A PC tries to get an IP address via dhcp-snooping, but it can't get IP successfully.

LSOD05565

- First Found-in Version: V3.03.00e
- Condition: Enable "dhcp-snooping" on a stack, and enable the downlink port serve as link-aggregation, and the member ports of link-aggregation are not on the same unit, the master port of the link-aggregation is down.
- Description: PC serves as DHCP client, requests ip via dhcp-snooping, and the PC can't get IP successfully.

LSOD05630

- First Found-in Version: V3.03.00e
- Condition: “Voice VLAN legacy” is enabled on a device.
- Description: When the CPU usage rate is high, the device maybe doesn’t send one CDP packet every second.

LSOD05840

- First Found-in Version: V3.03.00e
- Condition: Re-authentication is enabled on a RADIUS server, and certificate is used in the authentication process.
- Description: A user can't be re-authenticated successfully on a device.

LSOD05513

- First Found-in Version: V3.03.00e
- Condition: Configure a MD5 key longer than 16 bytes on a device and synchronize it with a NTP server through authentication. Then, save the configuration and reboot the device.
- Description: After rebooting, it can't be synchronized by the NTP server.

LSOD05807

- First Found-in Version: V3.03.00e
- Condition: In cluster view, try to reboot a member switch with its MAC address.
- Description: The member switch doesn't reboot.

LSOD06082

- First Found-in Version: V3.03.00e
- Condition: Run a command for selective QinQ when there isn't enough ACL resource.
- Description: The console freezes.

LSOD06122

- First Found-in Version: V3.03.00e
- Condition: Enable DHCP snooping and UDP-helper on a stack. DHCP client and DHCP server are connected to different device in the stack, and the MAC address of the DHCP client is static.
- Description: The DHCP client can't get an IP address successfully.

LSOD06072

- First Found-in Version: V3.03.00e
- Condition: EAD quick deployment is enabled on a device. A user and the predefined WEB server of EAD are connected to different VLAN.
- Description: If the user tries to access WEB through a browser before authentication, he maybe can't be redirected to the predefined page.

LSOD05415/LSOD05466

- First Found-in Version: V3.03.00e
- Condition: Enable port-isolate function on a link-aggregation.
- Description: Sometimes, the link-aggregation can't be isolated from the other ports in the isolate-group.

LSOD04221

- First Found-in Version: V3.03.00e
- Condition: Enable VLAN-VPN and mac-address-mapping on a port, and there is a loop under that port.

- Description: The devices under that port can't ping current device successfully even if the loop is broken.

LSOD04720

- First Found-in Version: V3.03.00e
- Condition: Configure burst-mode function on a 28-port device, in which a chip of 0xC0 version is used. (Note: The chip version can be seen through command "display drv soc_ver". If the output information is "The Version of switching chip is 0xC0.", then the chip version is 0xC0.)
- Description: The device doesn't respond, and can't be operated any more.

LSOD00656

- First Found-in Version: V3.03.00e
- Condition: WEB authentication is enabled on a port.
- Description: Multicast packets can pass through the port and create multicast group even if those packets aren't authenticated successfully.

LSOD00851

- First Found-in Version: V3.03.00e
- Condition: Fabric system configured as DHCP server, when lots of client request IP-address while system memory usage is up to 90%,
- Description: Master unit maybe reboots with deadloop.

LSOD02142

- First Found-in Version: V3.03.00e
- Condition: Configure a port with TPID non-0x8100
- Description: The port cannot tunnel BPDU packets, such as STP, LACP and HGMP.

LSOD02302

- First Found-in Version: V3.03.00e
- Condition: In a stack with link-aggregation across unit, the STP status transfers from forwarding to discarding by changing the STP cost.
- Description: A transient loop appears .

LSOD02678

- First Found-in Version: V3.03.00e
- Condition: In a network with full instance, full VLAN, and lots of MAC-address in switch MAC table, change the STP instance status.
- Description: Stack topology maybe oscillates and cannot convergence.

LSOD02688

- First Found-in Version: V3.03.00e
- Condition: Voice VLAN and EAD Quick Deployment are enabled on the same port.
- Description: EAD quick deployment doesn't work.

LSOD02896

- First Found-in Version: V3.03.00e
- Condition: Enable the STP in the fabric system and the system has learned full ARP entries in the port A. If the port A receives the TC packets, the ARP entries learned in the port A should be all deleted.
- Description: Only the ARP entries in the unit which includes the port A can be deleted, the ARP entries in other units can not be deleted completely.

LSOD03647

- First Found-in Version: V3.03.00e
- Condition: First enable the STP in a stack and configure the full instance and VLAN. And there are a lot of ports used in the stack. Save the configuration and reboot the stack manually.
- Description: The stack maybe reboots because of dead loop.

LSOD05051

- First Found-in Version: V3.03.00e
- Condition: The IRF system receives a lot of packets for a long time, at the same time many ports are up and down.
- Description: The IRF system may be split in probability.

LSOD06744

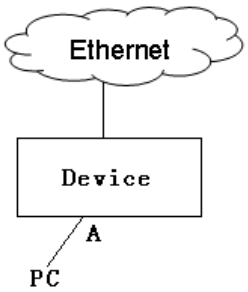
- First Found-in Version: V3.03.00e
- Condition: DHCP snooping is enabled on a device, and the device is synchronized by an NTP server.
- Description: After the device clock is synchronized, DHCP snooping records maybe ages quickly, so that user can't access network.

LSOD06581

- First Found-in Version: V3.03.00e
- Condition: Several users get limited privilege through EAD quick deployment first, then try to do EAD authentication.
- Description: If there aren't enough ACL rules available for EAD authentication, then those users can pass the EAD authentication, but some of them can't get the full privilege.

LSOD06207

- First Found-in Version: V3.03.00e
- Condition:



- Configure 802.1x on port A who does not do authentication on the device. Configure the PC MAC as static MAC on port A.
- Description: The PC with static MAC can't succeed in getting IP from DHCP server.

LSOD06877

- First Found-in Version: V3.03.00e
- Condition: Configure 802.1x on the device. Do authentication with DRCOM client.
- Description: Some times the EAPOL start packets from client get no response, authentication can't succeed. Once authentication succeeds, client can't log off, for the EAPOL logoff packet from the client get no response.

LSOD06858

- First Found-in Version: V3.03.00e
- Condition: Add a group of aggregation ports to a VLAN, and then enable ARP inspection function of the VLAN.
- Description: When change the relationship between the aggregation master port and the VLAN, i.e, remove the master port of the aggregation from the VLAN, system-configured ACL rules does not synchronize among the aggregation ports.

LSOD06820

- First Found-in Version: V3.03.00e
- Condition: Add a group of aggregation ports to a VLAN, and enable ARP inspection function of this VLAN. Shut down the master port of the aggregation.
- Description: ARP request packets come from the slave port of the aggregation will be broadcast back from original slave port.

LSOD06826

- First Found-in Version: V3.03.00e
- Condition: ARP inspection function is enabled of a VLAN (e.g. vlan10), and there is a dynamic DHCP snooping item (e.g. client A) in a port which belongs to the VLAN (vlan10). And also the client dynamic ARP item (client A) is learned.
- Description: Inject packets with spurious source MAC address from another port which makes station MAC movement event. Then the legal ARP item (client A) will be cheated to incorrect port and ARP inspection feature is malfunctioned.

LSOD05492

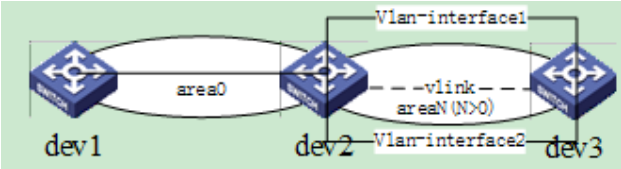
- First Found-in Version: V3.03.00e
- Condition: Set the min length of super user's password1 to N1,set a password which length is N2. Then change the min length of super user's password to N3(N3>N2≥N1).
- Description: The password1 still can log in.

LSOD06871

- First Found-in Version: V3.03.00e
- Condition: Use tftp source-ip command to set source-ip
- Description: That operates successfully on CLI, but failed on WEB.

LSOD06384

- First Found-in Version: V3.03.00e
- Condition:



1) dev1 connects dev3 through one VLAN interface, it locate area0, dev2 connects dev3 through two VLAN interface, they locate areaN (N>0);
2) The routes from dev3 to loopback address on dev2 are equal-cost routes;
3) Configure vlink peer on dev2 and dev3, set up two vlink neighbors between dev2 and dev3.

- Description: Use command display ospf peer brief to check the vlink neighbors' info: the address of the neighbors is not corresponding with address of the interface to the peer.

LSOD06672

- First Found-in Version: V3.03.00e
- Condition: A traffic-priority rule which filters packets with a range of source MAC-addresses are applied to a port (named as port-A). Then configure those MAC-addresses in the same range as OUI MAC-address.
- Description: Executing command copy configuration source port-A destination port-B will be failed. If port-A belongs to an aggregation group, the traffic-priority rule of port-A can't be synchronized to other port members in the same aggregation group.

LSOD06822

- First Found-in Version: V3.03.00e
- Condition: Enable DHCP snooping function on the switch; and connect a client to the switch through a HUB which is working on 10M speed and half duplex mode. Let the client do DHCP request operation frequently, and shutdown the port, which connects to HUB, on the switch.
- Description: Sometimes, there is no link-down trap prompted though the physical link is down. And the speed and duplex mode, showed by display interface command, will not be showed as "Unknown-speed mode, unknown-duplex mode".

LSOD06786

- First Found-in Version: V3.03.00e
- Condition: STP is disabled. Configure port isolate between Port A and Port B on one device. STP packets flow into Port A.
- Description: Port isolate fails, packets could be transmitted to Port B.

LSOD06487

- First Found-in Version: V3.03.00e
- Condition: Run command "ping -t" to ping link-part for a long time, the link-partner doesn't response in time. Thus, "request timeout" occurs.
- Description: After the link-partner resumes response, the device still can't ping the link-partner successfully. Only when the device run command "ping" again, it can ping the link-partner successfully.

LSOD06739

- First Found-in Version: V3.03.00e
- Condition: Dot1x and EAD Quick-Deploy are enabled on device. Dot1x is enabled on port A. Send a lot of packets with unknown source MAC to port A.
- Description: Memory leak.

Resolved Problems in V3.03.00e

It is the first release of V3.03.xx.

Related Documentation

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

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

Software Upgrading

The device software can be upgraded through console port, TFTP, and FTP.

Remote Upgrading through CLI

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

```
<Switch> ftp 10.10.110.1
Trying
Press CTRL+K to abort
Connected
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User(none):lyt
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get switch.app switch.app
[ftp] get switch.btm switch.btm
[ftp] bye
<Switch> boot bootrom switch.btm
please wait ...
 Bootrom is updated!
<Switch> boot boot-loader switch.app
<Switch> display boot-loader
The app to boot at the next time is: flash:/ switch.app
<Switch> reboot
```

After getting the new application file, reboot the device to have the upgraded application take effect.

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

The following sections introduce some approaches to local upgrading.

Boot Menu

After powering on the switch, run the Boot ROM program first, and the terminal screen will display the following information:

```
Starting......

      ******************************************************************
      *                                                                *
      *  Switch 5500 PWR 28-Port BOOTROM, Version 3.01                 *
      *                                                                *
      ******************************************************************

      Copyright (c) 2004-2007 3Com Corporation and its licensors.
      Creation date   : Nov 27 2007, 11:54:20
      CPU type        : BCM4704
      CPU Clock Speed : 200MHz
      BUS Clock Speed : 33MHz
      Memory Size     : 64MB

      Mac Address     : 000fe2123456

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

Press <Ctrl+B> to access the Boot menu.

Note

To access the Boot menu, press <Ctrl+B> within 5 seconds after the screen prompts “Press Ctrl-B to enter Boot Menu...” Otherwise, the system will start executing the program decompression. At this time if users want to access the Boot menu, they will have to reboot the switch.

The system prompts:

```
Password :
```

Enter the Boot ROM password. After entering correct password (no password is set for the switch by default), the system will access the Boot menu.

Caution

Please keep in mind the modified Boot ROM password.

```
          BOOT  MENU

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

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

Software Upgrading via Console Port (Xmodem Protocol)

Step 1: Enter **6** in the Boot menu. Press <Enter> and the system will access the download program menu.

```
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 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. Exit
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 **Error! Reference source not found.**) and select the software to be downloaded. Change the protocol name to Xmodem.

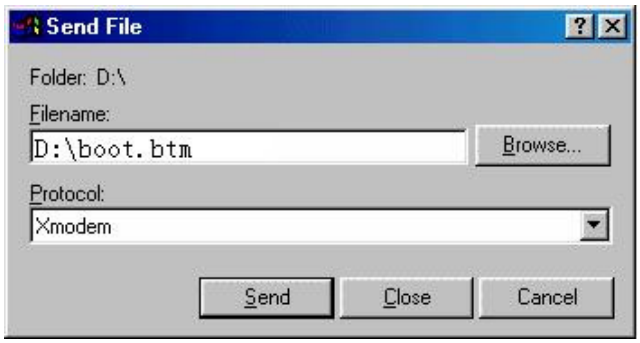


Figure 1 Send File

Step 6: Click <Send> and the system will display the window as shown **Error! Reference source not found.**.

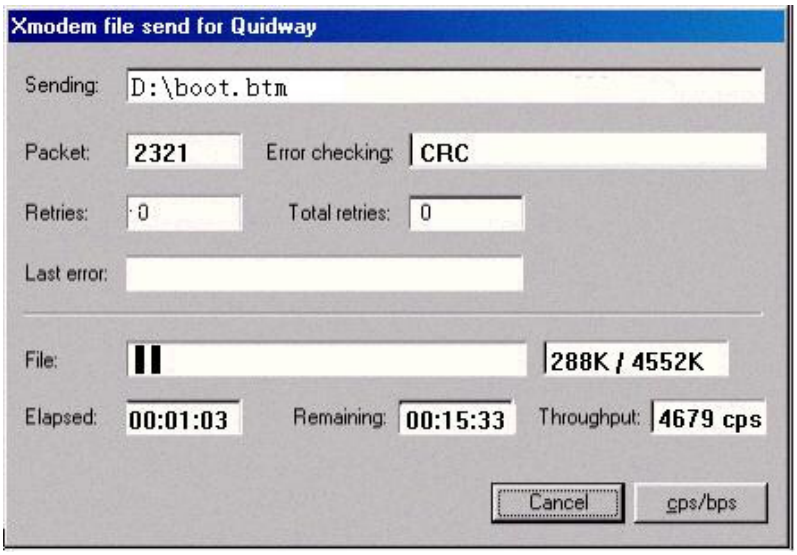


Figure 2 Xmodem File Send

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

```
Loading ...CCCCCCCCCC 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 S900. 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

Please keep in mind the modified Boot ROM password.

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:

```
Load File name

Switch IP address  (This address and the server IP address must be on the same network
segment)

Server IP address   (IP address of the PC where the file is stored)
```

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 5500 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 5500 serves as an FTP client.

2) FTP upgrading procedure

Step 1: Select an Ethernet interface for downloading on the 5500. 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!
```