# Release Notes for 200, 300, 500, and ESW2 Series Switches Software Version 1.3.x

**July 2013**

These Release Notes describe the recommended practices and known issues that apply to the Version 1.3.x software for products listed in the table below.

**NOTE** Firmware version 1.3.2 contains updates to products in the Sx200 Series only and introduces four new product models SF200-24FP, SG200-10FP, SG200-26FP, and SF200-24. Version 1.3.2 does not differ from firmware version 1.3.0 in any other way.

| Model | Description | Ports |
|---|---|---|
| SF200-24FP | 24-Port 10/100 PoE Smart Switch | e1-e24, g1, g2 |
| SG200-10FP | 10-Port Gigabit PoE Smart Switch | g1-g10 |
| SG200-26FP | 26-Port Gigabit PoE Smart Switch | g1-g26 |
| SG200-50FP | 50-Port Gigabit PoE Smart Switch | g1-g50 |
| SF200-24 | 24-Port 10/100 Smart Switch | e1-e24, g1-g2 |
| SF200-24P | 24-Port 10/100 PoE Smart Switch | e1-e24, g1-g2 |
| SF200-48 | 48-Port 10/100 Smart Switch | e1-e48, g1-g2 |
| SF200-48P | 48-Port 10/100 PoE Smart Switch | e1-e48, g1-g2 |
| SG200-18 | 18-port Gigabit Smart Switch | g1-g18 |
| SG200-26 | 26-port Gigabit Smart Switch | g1-g26 |
| SG200-26P | 26-port Gigabit PoE Smart Switch | g1-g26 |

| Model | Description | Ports |
|---|---|---|
| SG200-50 | 50-port Gigabit Smart Switch | g1-g50 |
| SG200-50P | 50-port Gigabit PoE Smart Switch | g1-g50 |
| SG300-10 | 10-port Gigabit Managed Switch | g1-g10 |
| SG300-10MP | 10-port Gigabit PoE Managed Switch | g1-g10 |
| SG300-10SFP | 10-port Gigabit PoE Managed Switch | 8 SFP + 2 Combo slots |
| SG300-10P | 10-port Gigabit PoE Managed Switch | g1-g10 |
| SG300-20 | 20-port Gigabit Managed Switch | g1-g20 |
| SG300-28 | 28-port Gigabit Managed Switch | g1-g28 |
| SG300-28P | 28-port Gigabit PoE Managed Switch | g1-g28 |
| SG300-28MP | 28-port Gigabit Max PoE Managed Switch | g1-g28 |
| SG300-52 | 52-port Gigabit Managed Switch | g1-g52 |
| SG300-52P | 52-port Gigabit PoE Managed Switch | g1-g52 |
| SG300-52MP | 52-port Gigabit Max PoE Managed Switch | g1-g52 |
| SF300-08 | 8-port 10/100 Managed Switch | e1-e8 |
| SF302-08 | 8-port 10/100 Managed Switch | e1-e8, g1-g2 |
| SF302-08MP | 8-port 10/100 PoE Managed Switch | e1-e8, g1-g2 |
| SF302-08P | 8-port 10/100 PoE Managed Switch | e1-e8, g1-g2 |
| SF300-24 | 24-port 10/100 Managed Switch | e1-e24, g1-g4 |
| SF300-24P | 24-port 10/100 PoE Managed Switch | e1-e24, g1-g4 |
| SF300-24MP | 24-port 10/100 Max PoE Managed Switch | e1-e24, g1-g4 |
| SF300-48 | 48-port 10/100 Managed Switch | e1-e48, g1-g4 |
| SF300-48P | 48-port 10/100 PoE Managed Switch | e1-e48, g1-g4 |

| Model | Description | Ports |
|---|---|---|
| SF500-24 | 24-port 10/100 Stackable Managed Switch | e1-e24, g1-g4<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP) |
| SF500-24P | 24-port 10/100 PoE Stackable Managed Switch | e1-e24, g1-g4<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP) |
| SF500-48 | 48-port 10/100 Stackable Managed Switch | e1-e48, g1-g4<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP) |
| SF500-48P | 48-port 10/100 PoE Stackable Managed Switch | e1-e48, g1-g4<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP) |
| SG500-28 | 28-port 10/100/1000 Stackable Managed Switch | g1-g28<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP) |
| SG500-28P | 28-port 10/100/1000 PoE Stackable Managed Switch | g1-g28<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet+ 2 1GE/5GE SFP |
| SG500-52 | 52-port 10/100/1000 Stackable Managed Switch | g1-g52<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP) |
| SG500-52P | 52-port 10/100/1000 PoE Stackable Managed Switch | g1-g52<br>4 Gigabit Ethernet (2 combo* Gigabit Ethernet+ 2 1GE/5GE SFP) |
| SG500X-24 | 24-port 10/100/1000 Stackable Managed Switch | g1-g24, xg1-xg4<br>4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules) |

## Release Notes

| Model | Description | Ports |
|---|---|---|
| SG500X-24P | 24-port 10/100/1000 PoE Stackable Managed Switch | g1-g24, xg1-xg4<br>4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules) |
| SG500X-48 | 48-port 10/100/1000 Stackable Managed Switch | g1-g48, xg1-xg4<br>4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules) |
| SG500X-48P | 48-port 10/100/1000 PoE Stackable Managed Switch | g1-g48, xg1-xg4<br>4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules) |
| ESW2-350G-52DC | 52-port Gigabit Managed Switch | g1-g52 |
| ESW2-550X-48DC | 48-port 10/100/1000 Stackable Managed Switch | g1-g48, xg1-xg4<br>4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules) |

**NOTE** *For the Sx500 Series, each combo mini-GBIC port has one 10/100/1000 copper Ethernet port and one mini-GBIC/SFP Gigabit Ethernet slot, with one port active at a time.

These caveats apply to:

SW version: 1.3.0 (1.3.0.62)

ESW2 Boot version: 1.2.9.01

Sx500 Boot version: 1.2.0.12

**NOTE** The boot version for the ESW2 and Sx500 devices is new. It must be upgraded in order to support the new hybrid stacking feature.

Sx300 Boot version HW V01: 1.0.0.4

Sx200 Boot version HW V01: 1.0.0.1

Sx300 Boot version HW V02: 1.1.0.6

Sx200 Boot version HW V02: 1.1.0.6

**TIP** As with any firmware release, please read these release notes before upgrading the firmware. Cisco also recommends backing up your configuration before any firmware upgrade.

# Contents

Hardware Versions, page 6

Major Changes and Defects Corrected, page 8

Limitations and Restrictions, page 10

Where to Find Support, page 18

# Hardware Versions

The Release 1.3.0.62 firmware runs on two different versions of hardware for the 200 Series Smart Switches, and the 300 Series Managed Switches. There is a single version of hardware for the 500and ESW2 series switches. The number of supported MAC Addresses, Active VLANs, and Multicast Groups will be different depending on which version of hardware you are using. Refer to the following table for details:

| V1 versus V2 Hardware | Total Number of MAC Addresses | Total Number of Active VLANs | Total Number of Multicast Groups |
|---|---|---|---|
| Sx200 in Firmware 1.0.x HW VID=01 | 8K | 128 | 128 |
| Sx200 in Firmware 1.1.x and above. HW VID=01 | 8K | 256 | 256 |
| Sx200 in Firmware 1.1.x and above. HW VID=02 | 8K | 256 | 256 |
| Sx300 in Firmware 1.0.x HW VID=01 | 8K | 256 | 256 |
| Sx300 in Firmware 1.1.x and above. HW VID=01 | 8K | 256 | 256 |

| V1 versus V2 Hardware | Total Number of MAC Addresses | Total Number of Active VLANs | Total Number of Multicast Groups |
|---|---|---|---|
| Sx300 in Firmware 1.1.x and above.<br>HW VID=02 | 16K | 4K | 1K |
| Sx500, SG500X and ESW2 switches have a single version of HW, see the admin guide for details. | | | |

To determine which version of hardware you are using, click **Status > System Summary**. Look at the lower portion of the screen under the graphic representation of the switch for the PID VID. The descriptor will end in the VID number. The version information is also shown on the product label on the back of the switch. The PID VID is located at the bottom of the label.

# Major Changes and Defects Corrected

## Major Changes

- Added support for RMON History, Events and Alarms for the 200 Series Switches.
- Added Basic Hybrid and Advanced Hybrid modes for stacking. Increased the number of units in a Hybrid stack up to 8.
- Added Unicast SNTP Server time synchronization.
- Added the SCP option for the 200 Series Switches.
- Reorganized the web-based administration by adding the System Object ID and SNMP Service to the Sx300 System Summary page in System Information. Removed the TCAM Allocation page and added the Router Resources page.
- Added several IPv6 improvements. Added IPv6 Support for TACAS+, Telnet server, DHCPv6 Client, and DHCPv6 Relay.
- Added support for SNMP and SSH Client to the 200 Series Switches.
- Updated DSCP to Queue to 8 queues where relevant.
- Added DHCPv4 Server
- Static IPv6 Routing on the 500 series has been added.
- Increased the number of LAG interface from 8 to 32 on 500 Series.
- Firefox 4 to 10, Internet Explorer 7 to 9, Safari Browser 5-6, and Chrome Browser 14-15 are supported.

## Defects Corrected

- The system cannot access Management IP successfully after the switch is reset to default, and the IP address is set as static 192.168.1.254. If any other static IP addess is confirgured, there is no problem. (CQ147364)
- The firmware MD5 Checksum is missing while executing “show version md5” command through CLI. (CQ147303)
- In GUI, if two same ACE are created on one ACL, for example: ip access-list permit any, then deleting one of the ACE will cause the DUT to crash. This

issue does not occur on the CLI, because the CLI will not permit two ACE to be created on one ACL. (CQ147329)

- After a static IPv4 route is configured on Sx300, this route is not displayed on WEB GUI though this route works fine. However, it can successfully be displayed in CLI, and it does not matter whether this route was created via CLI or GUI. (CQ147056)
- After the firmware is upgraded from 1.2.9.44 to 1.3.0, the IP default gateway changes to default route. (CQ146158)
- In the router mode and default configuration, whenever the DHCP IP address is renewed, the previous entry in the table is not removed. After a while the following message is displayed – "17-Apr-2013 06:51:03 :%ARP-E-ARPTBL: ARP Table Overflow", and the TCAM is exhausted. (CQ147161)

# Limitations and Restrictions

## The following caveats are acknowledged in release 1.3.0.62:

**Problem:** In switch mode although multiple default gateways can be configured through CLI, only the gateway with lowest value can be active. Hence, switches should not allow the CLI to configure multiple default gateways.

**Solution:** When modifying the default gateway through CLI, delete the old one first. (CQ147302)

**Problem:** In web GUI “Security->Arp Inspecties->Properties”, the “DHCP Snooping Binding database” hyperlink is invalid.

**Solution:** Access it through “IP Configuration-> DHCP-> DHCP Snooping Binding Database”. (CQ147363)

**Problem:** When the firmware is downgraded from 1.3.0.62 to 1.2.9.44, the IP static routes are lost.

**Solution:** Configure static route again after downgrade to previous release. (CQ147578)

**Problem:** When the value of the SA or DA is changed from a valid MAC to any other value in the webpage, the SA or DA becomes 0000.0000.0000 in CLI.

**Solution:** Delete ACL and configure again. (CQ147665)

**Problem:** In web GUI “Security->IP Source Guard->Properties”, the “DHCP Snooping” hyperlink is invalid.

**Solution:** Access it through “P Configuration-> DHCP Snooping/Relay”. (CQ147666)

**Problem:** In web GUI “Security->IP Source Guard->Interface”, the “DHCP Snooping” and “DHCP Snooping untrusted interfaces” hyperlinks are invalid.

**Solution:** Access them through “IP Configuration-> DHCP Snooping/Relay”. (CQ147667)

## The following caveats are carried forward from release 1.3.0.59:

**Problem:** Some of the pages in the web-based interface require the Java Runtime Environment (JRE) to be installed, otherwise they may display incorrectly.

**Solution:** Install the latest JRE.

**Problem:** Granularity of traffic shaping on the following Uplink ports starts with 2Mbps and not with 64Kbps. When configuring traffic shaping on these ports to rates lower than 2Mbps, the actual traffic shaping rate will be 2Mbps. (CQ123397, CQ130715, CQ133170)

- Sx200/Sx300 HW 1.0
- SF500 ports GE1-GE4
- SG500 ports GE-49 - GE52
- SG500X ports XG1 - XG4

**Solution:** Use the specified ports when traffic shaping is not required (for example. uplink or stack ports), or when the required traffic shaping rate is at least 2Mbps.

**Problem:** When the link on the SG500X ports XG1 - XG4 uplink ports comes up, the link may go up and down a few times then stabilize on the up state. (CQ135073)

**Solution:** There is no workaround.

**Problem:** After frequent changes of the stack topology from ring to chain and vice versa, one of the stack links might become non-operational (stuck in a state where even if the stack topology is ring, it will function as a chain). If the remaining operational stack link goes down, the stack might become non-operational. (CQ135108)

**Solution:** Wait for the stack to stabilize before changing its topology.

**Problem:** Copper SFP MGBT1 is not supported as stack port due to packet loss and bad CRC. (CQ135473)

**Solution:** Use Cisco approved SFPs.

**Problem:** When a PoE switch is connected to another PoE switch, one of the switches overcomes the internal power supply of the other PoE switch, so the other PoE switch cannot provide PoE power to powered devices. If the connection between these switches is removed, the switch that received power from the other switch will momentarily lose its power and reboot. (CQ135360, CQ138875)

**Solution:** Disable PoE on the ports connecting the two PoE switches.

**Problem:** Given a stack configuration with the stack master as unit #2. On the Port Vlan Membership page of the web-based interface, changing the value on the Interface Type drop-down, the drop-down returns to unit #1. The information displayed on the rest of the page belongs to the ports of the unit that was selected using the drop-down. (CQ141909)

**Solution:** There is no workaround.

**Problem:** The routing resource "Used number of hosts" is not displayed correctly. This is just a display issue, there is no user impact. (CQ133802)

**Solution:** There is no workaround.

**Problem:** In Layer 3 mode, SNTP Broadcast can only be operated from the CLI.

**Solution:** There is no workaround.

**Problem:** The EEE operational status should become disabled when Auto Negotiation is disabled. (CQ132106 )

**Solution:** When the speed on a port is 1 Gigabit, auto negotiation has no effect on the EEE functioning state.

**Problem:** The Voice VLAN should be prevented from being set as Guest VLAN, and the user should receive a warning. This is not happening. (CQ132684)

**Solution:** Avoid setting the Voice VLAN as guest VLAN and vice-versa.

**Problem:** When the Mrouter learning mode is changed between "user defined" to "auto" and vice-versa, the IGMP Querier election process does not start. (CQ132805)

**Solution:** Disable IGMP Snooping and re-enable again, every time the Mrouter learning mode is changed to start the Querier election process.

**Problem:** Some WEB GUI pages require full version compatibility of JRE, Browser and JRE-Browser applets. For XML compatibility reasons, MSXML DLL Version 6 is required for IE browser users.

**Solution:** For download and installation please refer the following link: **www.microsoft.com/downloads/details.aspx?FamilyID=993C0BCF-3BCF-4009-BE21-27E85E1857B1&displaylang=en**

**Problem:** Notification Recipients table entry becomes un-editable with an incorrect or missing parameter. (CQ133316)

**Solution:** There will be an asterisk by any values for a table entry which are incorrect. This can be caused by the deletion of users, views, etc. If any of these values are incorrect, then the entry will be un-editable. First add the missing user, view, etc, in order to edit the entry. The delete button still works regardless of whether the values are correct or not.

**Problem:** The result of cable length test for 100 meters is incorrect. It will show between 110 to 140 meters. (CQ132941)

**Solution:** There is no workaround.

**Problem:** The maximum number of IPv6 ACEs that can be applied on an interface is 244, not 512 as documented. The user receives the message “Cannot apply because of a lack of hardware resources.” (CQ130161)

**Solution:** There is no workaround.

**Problem:** If changing the active image with the menu CLI, the active image after reboot field is not updated. If you change the image number and reboot, then the image does change, but the display in the menu CLI is incorrect. (CQ132211)

**Solution:** There is no workaround.

**Problem:** When using the CLI, any time that DNS is used, the user is blocked from interacting with the CLI until the DNS lookup has completed. (CQ133234)

**Solution:** The user must wait until the DNS lookup has completed before issuing another command.

**Problem:** When a DVA authorized port tries to re-authenticate and RADIUS attributes no longer include VLAN attributes, reauthentication should fail and the port should become unauthorized. This is not happening, and the port does not fail. (CQ131469)

**Solution:** Do not remove VLAN attributes on a RADIUS server or unplug the network cable and plug it back in to force the failure.

**Problem:** Egress rate shaping does not work as expected. Configuring egress shape on Gigabit ports or on Combo ports between 64k to 5000k, will always result in 2 Million Bits. This is resolved with the new hardware release 1.1.1.8. It still exists on HW V01. It also does not work on SG300-52/52P & SG200-52/52P switches. (CQ123397 and CQ130715)

**Solution:** There is no workaround.

**Problem:** SNTP synchronization error messages are not logged when an incorrect MD5 key leads to the loss of synchronization. (CQ132636)

**Solution:** There is no workaround for broadcast messages. For Unicast servers, in the SNTP server table the status message will either say "In process" or "Down" for those servers that have failed authentication.

**Problem:** PoE ports on certain Nikola switches might not power the connected powered devices (PD) when used along with Cisco IP Phone 7960 with PID=68-0808-xx. This issue impacts the following switch models:
Switch SKUs: SG200-26P, SG200-50P, SG300-28P, SG500-28P, SG500-52P, SG500X-24P and SG500X-48P.

**Solution:** Use CAT 5 cables with with 2 pair pins 1, 2, 3, and 6.

**Problem:** When configuring egress shaping rates on port 1, and enable flow control on port2, the whole vlan port egress rates will be the same. Flow control uses the whole buffer management scheme. When one port is configured to FC ALL ports are applied by the new scheme. QoS function on other ports will be effected also. (CQ144583)

**Solution:** When using QoS, disable the flow control function.

**Problem:** You cannot configure IP address 192.168.1.0/24 subnet as an address pool, other subnets are allowed. (CQ145102)

**Solution:** There is no workaround.

**Problem:** The `show environment` command on a stack shows a temperature of 0 for all units if the switch without a sensor is the master in the stack. (CQ145525, CQ145542)

**Solution:** There is no workaround.

**Problem:** When managing a switch through the web-based interface, the loading time on some of the web pages can take a long time, approximately 3-10 seconds depending on the content in the tab. (CQ143850)

**Solution:** Use the command line interface instead.

**Problem:** When managing stacking switches through the web-based interface, the loading time on the following web pages is more than 10 seconds: (CQ143851)

- Status and Statistics
- Port Management
- VLAN Management
- Access Control
- Quality of Service

**Solution:** Use the command line interface instead.

**Problem:** When the current master unit is already set to auto-numbering, reconfiguring it as 'auto' does not work. (CQ142567)

**Solution:** Use the command line interface to configure this feature.

**Problem:** When configuring a manual IPv6 tunnel with EUI-64 format, the Global IPv6 address is not created. (CQ140132)

**Solution:** Do not use the EUI-64 format when configuring an IPv6 manual tunnel.

**Problem:** You cannot configure ipv6 tunnel parameters if you previously did not define the mode type. (CQ140919)

**Solution:** Configure the tunnel mode first when configuring an IPv6 tunnel.

**Problem:** You cannot run ping or traceroute by using a Domain Name on the web-based interface. (CQ143759)

**Solution:** Use the command line interface instead.

**Problem:** When you are prompted to modify your password at the initial log in, and then change the default password to use some special strings, the user will fail to log in again with the modified password. An example of special strings would be: like "Cisco100%+" or "WERab#%56". (CQ145271)

**Solution:** Use other passwords without special strings or use these strings as a password after changing the password at least one time.

**Problem:** It is impossible to configure more than 255 multicast groups on an Sx500 switch in Router Mode. The stated limit in the documentation is 1k multicast groups. (CQ143282)

**Solution:** There is no workaround.

**Problem:** There is a problem using PoE auto control via time-range. After performing a save and reboot, the saved time-range configuration on port 4 is also displayed on port 5 and 6. (CQ146121)

**Solution:** There is no workaround.

**Problem:** If you modify an IPv6 tunnel configuration, the change will not take effect until you perform a *shut* then *no shut* on the tunnel interface. (CQ146071)

**Solution:** You must perform a *shut* then *no shut* the tunnel interface for it to take effect.

**Problem:** The power inline server time-range function does not work. (CQ146048)

**Solution:** Use the power inline auto time-range function instead, but you will need to use an opposite time-range.

**Problem:** A global ipv6 address cannot be set in a tunnel interface when following specific steps using the web-based interface. (CQ146027)

**Solution:** Reconfigure using the web-based interface, or configure it using the command line interface.

**Problem:** When a 10G DAC (Direct Attached Cable) is connected to the copper port of the SG500 using the last two ports (combo ports), the fiber link status display might be up even when the link is not active. (no defect number)

**Solution:** There is no workaround.

**Problem:** Occasionally, a TACACS server that has been configured by using a name cannot be deleted. (CQ146164)

**Solution:** Configure a TACACS server by IP address.

**Problem:** When enabling IPv6 unicast-routing, the interface cannot get an ipv6 address via auto-config. (CQ146156)

**Solution:** Configure the interface using a static IPv6 address.

**Problem:** When configuring a 500 series switch in L3 mode, the user is allowed to configure the TCAM for IP4 and IPv6 routing resource on the same web page. (CQ146267)

The issue occurs on the backup switch in a stack. Refer to the following steps as an example:

**STEP 1** Open the **Administration > Routing Resources** page.

**STEP 2** Adjust the IPv6 entry from the default value to 8, then apply and reboot the switch to take effect.

**STEP 3** After the switch boots up, configure IPv4 entry to 1800, then apply and reboot.

**STEP 4** The backup switch will reboot repeatedly, other stack members work as expected.

**Solution:** Adjust the IPv4 and IPv6 router resources at the same time. To recover the backup switch, you need to press the reset button for 10 seconds to return it to factory defaults.

## Japanese language files and firmware version compatibility guideline

Users will see a mismatch in the features between the English language and the Japanese language when running certain combinations of firmware and language files. Users will see new features added since version 1.1.1.6 in English instead of Japanese in the GUI when running firmware version 1.1.2.0 and higher subject to the following restriction:

- Japanese language files version 1.1.1.6 and older are forward compatible up to Firmware version 1.1.2.0. For example: loading a version 1.1.1.6 language file onto a device running firmware version 1.2.7.76 and up will fail.
- Japanese language files version 1.1.1.10 and newer are only compatible with firmware version 1.2.7.76 and newer.

# Where to Find Support

To obtain current support information for Cisco Small Business products, visit the following URLs:

www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/500_series_switches/index.html

www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/300_series_switches/index.html

www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/200_series_switches/index.html

www.cisco.com/go/smallbizsupport



78-21240-02