

# Release Notes for 200, 300, 500, and ESW2 Series Switches Software Version 1.3.5.x

**October 2013**

These Release Notes describe the recommended practices and known issues that apply to the Version 1.3.5.x software for the following products:

Model	Description	Ports
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
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
SG300-10MPP	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

## Release Notes

Model	Description	Ports
SG300-10PP	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
SG300-28PP	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
SF302-08PP	8-Port 10/100 PoE+ Managed Switch	e1-e8, g1-g2
SF302-08MPP	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
SF300-24PP	24-Port 10/100 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
SF300-48PP	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 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 4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP)
SF500-48	48-port 10/100 Stackable Managed Switch	e1-e48, g1-g4 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 4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP)
SG500-28	28-port 10/100/1000 Stackable Managed Switch	g1-g28 4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP)
SG500-28P	28-port 10/100/1000 PoE Stackable Managed Switch	g1-g28 4 Gigabit Ethernet (2 combo* Gigabit Ethernet+ 2 1GE/5GE SFP)
SG500-28MPP	28-Port Gigabit PoE+ Stackable Managed Switch	g1-g28 4 Gigabit Ethernet (2 combo* Gigabit Ethernet+ 2 1GE/5GE SFP)
SG500-52	52-port 10/100/1000 Stackable Managed Switch	g1-g52 4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP)
SG500-52P	52-port 10/100/1000 PoE Stackable Managed Switch	g1-g52 4 Gigabit Ethernet (2 combo* Gigabit Ethernet+ 2 1GE/5GE SFP)

## Release Notes

Model	Description	Ports
SG500-52MP	52-Port Gigabit PoE+ Stackable Managed Switch	g1-g52 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 4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules)
SG500X-24P	24-port 10/100/1000 PoE Stackable Managed Switch	g1-g24, xg1-xg4 4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules)
SG500X-48	48-port 10/100/1000 Stackable Managed Switch	g1-g48, xg1-xg4 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 4 10 Gigabit Ethernet SFP+ (1/5/10GE SFP+ modules)
SG500XG	16-Port 10-Gigabit Stackable Managed Switch	xg1-xg16 16 10GE ports (8 copper ports and 8 fiber ports) + 1GE port
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 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: 1.3.5 (1.3.5.56)

ESW2 Boot version: 1.3.5.06

Sx500 Boot version: 1.3.5.06

**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: 1.3.5.06

Sx200 Boot version HW V01: 1.3.5.06

Sx300 Boot version HW V02: 1.3.5.06

Sx200 Boot version HW V02: 1.3.5.06

**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 12](#)

[Where to Find Support, page 22](#)

## Hardware Versions

The Release 1.3.5.x 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 500 and 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. 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

### Change in Flash file system

- In version 1.3.5, the Flash file system was upgraded. This has implications when upgrading from previous releases to version 1.3.5, and when downgrading from 1.3.5 version to previous versions as described below.

#### *Upgrading from previous releases*

During the first bootup of the new version, the flash file system is upgraded. Note that:

- This process takes a few minutes. “...” progress in the Console will be displayed during this process (not relevant to Sx200).
- The syslog file is deleted during this process.
- The original image file is deleted. The two images on the Flash after the upgrade will have the same version (1.3.5).

**NOTE** Before upgrading to version 1.3.5, the boot loader also needs to be updated. If version 1.3.5 is installed using the original boot loader, the file system will not be upgraded, and in the future the user will not be allowed to upgrade to versions higher than 1.3.5.

#### *Downgrade from 1.3.5 to previous releases*

- The downgrade copy operation process takes a few minutes since the file system needs to be converted prior to the copy operation itself. The user will be notified (using “.....” progress on CLI or a message on the WEB GUI) that the conversion process is ongoing. When the conversion process ends, the image download begins automatically. The device will automatically reboot after the copy is finished.

**NOTE** Powering off the device during this process might damage the file system, in such case, booting up might require connecting to the device using the console cable (not relevant to Sx200) and loading the image file using XMODEM.

- After the downgrade, only downloaded image file will remain on the Flash (the 1.3.5 image is deleted during this process). Note that there's no need to downgrade the boot file, the boot file supports both file systems. The boot file cannot be downgraded while version 1.3.5 is active.



### Other Changes

- Added new feature, UDLD (Uni-Directional Link Detection), which discovers Uni-Directional links for Sx300 and Sx500.
- Added new feature IPv6 First Hop Security, which is a suite of features designed to secure link operations in an IPv6 network for Sx300 and Sx500.
- Introduced a Loopback Interface which is a virtual interface whose status is always up. The user can specify, per feature, whether the source interface from which IP traffic is generated will be automatically selected by the system or user defined (user-defined can be loopback interface or any other interface).
- Updated 802.1X to add support for Web-Based Authentication (Captive Portal) on the Sx300, Sx500, SG500X and SG500XG. Added ability to define the maximum number of authorized hosts per interface. In MAC Based Authentication, a port does not have to be a member of the guest VLAN, and re-authentication does not have to be enabled on the port. Dynamic VLAN Assignment can be enabled in all the host modes (Single/multiple host, multiple session); in case the Radius reply does not contain the VLAN attribute, the user can specify whether the authentication will fail or not. In Multi-session mode, Guest VLAN exists on the port even after a client was authenticated.
- Updated DHCP Server to add support for user-defined options for Sx300 and Sx500.
- Added option of Auto-Recovery of disabled interfaces. After the system shuts-down an interface (errDisable), it can be automatically recovered after a specified elapsed time.
- Updated PoE to add an option to skip the inrush test (for supporting non-standard devices). In Port limit mode, the power limit does not take the PoE class of the connected device into account.
- Updated SNMP Traps to add an option to disable link up/down SNMP traps.
- Added the Exec Banner which is a banner that is displayed after successful login.
- Added VLAN Shutdown which stops L3 traffic on specific VLAN.
- Modified the location of the Help files. The help files, which were located on the device Flash memory in previous releases, are now located on Cisco.com website.

- Modified VLAN ACL such that an ACL can now be attached to a VLAN, and not only to port/LAG for Sx300 and Sx500.
- Updated Show system so that the system type (e.g. SG500X-24P) is added to the System Description field in the output of this CLI command for Sx300 and Sx500.
- Updated LLDP so that the sysName TLV is sent by default. Chassis ID can be either MAC Address (as in previous releases) or Hostname.

### Defects Corrected

- In web GUI “Security->Arp Inspection->Properties”, the “DHCP Snooping Binding database” hyperlink is invalid. (CQ147363)
- When the firmware is downgraded from 1.3.0.62 to 1.2.9.44, the IP static routes are lost. (CQ147578)
- 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. (CQ147665)
- In web GUI “Security->IP Source Guard->Properties”, the “DHCP Snooping” hyperlink is invalid. (CQ147666)
- In web GUI “Security->IP Source Guard->Interface”, the “DHCP Snooping” and “DHCP Snooping untrusted interfaces” hyperlinks are invalid. (CQ147667)
- 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)
- You cannot configure IP address 192.168.1.0/24 subnet as an address pool, other subnets are allowed. (CQ145102)
- 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)
- When the current master unit is already set to auto-numbering, reconfiguring it as 'auto' does not work. (CQ142567)
- You cannot run ping or traceroute by using a Domain Name on the web-based interface. (CQ143759)

- 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)
- 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)
- The power inline server time-range function does not work. (CQ146048)
- A global ipv6 address cannot be set in a tunnel interface when following specific steps using the web-based interface. (CQ146027)
- Occasionally, a TACACS server that has been configured by using a name cannot be deleted. (CQ146164)
- 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:
  1. Open the **Administration > Routing Resources** page.
  2. Adjust the IPv6 entry from the default value to 8, then apply and reboot the switch to take effect.
  3. After the switch boots up, configure IPv4 entry to 1800, then apply and reboot.
  4. The backup switch will reboot repeatedly, other stack members work as expected.

# Limitations and Restrictions

### The following caveats are acknowledged in release 1.3.5.x:

**Problem:** On SG500XG-8F8T switches, 1000BASE-T and 100BASE-TX modes only support frame sizes up to 9000 bytes. If the 10G copper port is configured in the 1G or 100M mode, and oversized frames are sent, the port drops the link. Shutting and then opening this port can bring up this port again. (CQ149642, CSCuj46378)

**Solution:** Limit frame size to 9000 bytes or less in 1000BASE-T mode.

**Problem:** For the SX500 and SG500X switches, when users manually assign the unit ID, and at the same time force units 1 or 2 to be the stack master, the unit shuts down when the unit is reloaded. (CQ150107, CSCuj46520)

**Solution:** Reloading or Power cycling all units in stack will resolve the problem.

**Problem:** On the SX500 and SG500X switches, when the users modify the unit ID, and force master selection at the same time, the stack master shuts down. (CQ150148, CSCuj38655)

**Solution:** Configure the unit ID on the web GUI. Reload the stack and converge, and then specify force master. While reloading the switch, configuring it with a unique unit ID can recover the switch.

**Problem:** For SX500 stacking, when the stack mode is changed from native to basic hybrid using the command: stack basic-hybrid auto unit-id-auto reboot, and the stack is reloaded then restarted with the default configuration, the startup configuration file is removed. (CQ150131, CSCuj37279)

**Solution:** Backup startup-config file before changing the stack mode.

**Problem:** When authenticating using WBA, if too many HTTP sync packets are received within a short time, the login window is not displayed. The HTTP packets that arrive into authenticated port are not taken into account. The higher the number of HTTP sync packets received at the same time, the more difficult it is to open the login window. Usually, hundred HTTP sync packets received per second interrupt WBA service. (CQ149646, CSCui73779)

**Solution:** Continue to refresh web browser or stop the HTTP sync flood.

**Problem:** When the Chinese localization file is installed on the SX500 stack master from TFTP on the web GUI, and the stack cable between master and backup unit is removed, the localization file is not installed on the backup unit. If CLI is used, or if the file is copied through http, this issue is not observed. (CQ150000, CSCuj46533)

**Solution:** Use HTTP to install localization file.

**Problem:** When the firmware is upgraded from 1.3.0 to 1.3.5, both firmware images (active and non active) are saved as 1.3.5 in the flash memory. (CQ148800, CSCuj46557)

**Solution:** There is no workaround.

**Problem:** Sometimes LAG port cannot be up when using 1G SFP. This happens on SG500XG-8F8T and 10G SFP port. (CQ150142, CSCuj37498)

**Solution:** Keep the link up and reload the device.

**Problem:** Using the web GUI to edit the default port in the Neighbor Discovery Inspection Policy table takes more than 10 seconds. (CQ150135, CSCuj37395)

**Solution:** Configure using CLI.

**Problem:** When Maximal Router Preference set to No Verification on the web GUI, Minimal Router Preference cannot be configured. It displays a message stating "Maximal router preference verification level must be higher than or equal to the minimal router preference verification level". This issue is noticed only on the Web GUI. (CQ150108, CSCuj46567)

**Solution:** Configure using CLI.

**Problem:** When multiple resolved host names exist in web GUI, usually the last one or two entries cannot be deleted. (CQ149930, CSCuj46576)

**Solution:** Delete any of the above entries first, then delete last one or two entries.

**Problem:** When multiple different class PDs are connected to SF300-48PP, sometimes two or three ports are not delivered power although there is still power budget. This happens when Consumed Power is about 324 watt (86%) or more. (CQ147622, CSCuj46584)

**Solution:** There is no workaround.

**Problem:** The Stack Port LED on the System Summary page of the web GUI is inconsistent with front panel of SG500XG-8F8T. (CQ150109, CSCuj46594)

**Solution:** There is no workaround.

**Problem:** The VRRP Master and Backup status are switched when the Master VRRP preempt is turned-off. (CQ148375, CSCuh50815)

**Solution:** There is no workaround.

**Problem:** Users are unable to open IPv6 HTTP/HTTPS sessions on Apple Safari. (CQ147760, CSCuj46288)

**Solution:** Use Chrome or Internet Explorer.

**Problem:** UDLD is not working when port channel is configured on Fiber port. This issue is reported only for Fiber ports. (CQ147285, CSCuj46296)

**Solution:** There is no workaround.

**Problem:** When MAC-Based authentication or WEB-Based authentication is used, and the RADIUS server is configured to authentication methods (Multi auth-protocols) other than MD5 as the default method, authentication might fail. (CQ148263, CSCuh40196)

**Solution:** Configure the RADIUS server to use only MD5, or to prefer MD5 over the other configured methods.

**Problem:** SG500XG-8F8T does not support cable test on 10G and gigabit port. (CQ148165, CSCuj46301)

**Solution:** There is no workaround.

**Problem:** Sometimes SG500XG-8F8T 10G copper port goes up and down continuously if it is configured to a speed of 1G, and hence Lion stack performance have Losses of around 3% of frame loss. (CQ147378, CSCuj46317)

**Solution:** Configure Nikola switch ports in 1G speed to Auto-negotiation preferred master.

**Problem:** When storm control is enabled on a port, and the port speed is reduced to a lower speed, the storm control on the WEB GUI is displayed as disabled. (CQ149542, CSCui59739)

**Solution:** This is only a display issue. Refresh the WEB GUI storm control page. The status is displayed correctly.

**Problem:** It is possible to bind non-existent ACL and KEY chain to layer3 interface in web GUI, but the user can not edit or delete the entry in GUI. (CQ148424, CSCuh56676)

**Solution:** Delete the binding key chain or ACL from CLI.

**Problem:** When setting a new keychain for RIP using the WEB GUI, if it does not include an accept-lifetime, it does not take effect, and only Key 1 takes effect with accept-lifetime. (CQ148403, CSCuh54765)

**Solution:** Use the CLI for entering the keychain, or enter both accept-lifetime and send-lifetime. Only use Key 1 with accept-lifetime.

**Problem:** WRR will lose efficacy after it is configured to egress shaping rate. (CQ146677, CSCuf82588)

**Solution:** Configure the WRR again.

**Problem:** Enable password authentication does not work with ACS 5.4 Tacasc+. (CQ146266, CSCue93645)

**Solution:** Use ACS 4.X to enable password authentication.

**Problem:** When user tries to Telnet some other devices from switch, it takes a long time to logout. The user either needs to double click enter button or wait a long time to logout from the device and return to the switch. (CQ146113, CSCuj46177)

**Solution:** The only option is to either double click enter key or wait for a long time to logout.

**Problem:** Isatap tunnel lose efficacy after modify ISATAP tunnel configuration and hence cannot get ipv6 global address. (CQ146071, CSCuj52323)

**Solution:** Select Shutdown, and then no shutdown at the tunnel interface.

**Problem:** SG500XG-8F8T and SG500X can not be stacked together if using 1G SFP stack cable, and if the stack ports are configured at AUTO speed. (CQ149496, CSCui54965)

**Solution:** Set the stack ports to 1G speed, or connect the switches over a 10G Fiber connection.

**Problem:** On SG500XG-8F8T or SG500X, changing the stack mode from native to advanced-hybrid-xg causes the start-up configuration to be lost. (CQ148932, CSCui08988)

**Solution:** Backup startup-config file before changing the stack mode.

**Problem:** On SG500XG-8F8T, if the user enables short reach and show green-ethernet, the short reach operation always remains off. (CQ147929, CSCuj46182)

**Solution:** There is no workaround.

**Problem:** MAC-Based ACE work fails when ACE Entry Ethertype value is set to 8100. This is because MAC ACL which permit specific ethertype 8100 actually blocks the packets with ethertype 8100. This happens only on ethertype 8100. (CQ146317, CSCuj46199)

**Solution:** There is no workaround.

**Problem:** When two features are enabled on the same port, IP ACL affects Web based authentication function. The reason for this is, if port based IP ACL blocks DHCP, DNS or HTTP traffic, WEB based authentication cannot work. (CQ148890, CSCui06449)

**Solution:** Do not block DHCP, DNS or HTTP traffic if applying IP ACL on a WEB based authentication port.

**Problem:** When the switch is used as a DHCP server, it always assigns its IP address as default router option (option 3), even if this option is not configured in the DHCP pool. Even if any other IP address is configured, the switch will still continue to provide option 3 as the configured IP to the client. (CQ149277, CSCui34225)

**Solution:** There is no workaround.

**Problem:** When the firmware is downgraded from 1.3.5.39 to 1.3.0.62, only the image for 1.3.0 exists in flash. This happens on all platforms. (CQ148803, CSCuj46205)

**Solution:** Copy the required image to flash again.

**Problem:** On stacking, some WEB GUI pages respond slowly. If 8 switches are stacked and 200 devices are connected, some WEB GUI pages take more than 10 seconds to respond. (CQ137261, CSCuj46218)

Some examples of such WEB GUI pages are:

- LLDP Neighbor Information.
- VLAN Management Interface Settings
- 802.1X Port Authentication
- Quality of Service Bandwidth
- Quality of Service Egress Shaping Per Queue

**Solution:** Wait until the WEB GUI pages respond or use CLI commands.



## The following caveats are carried forward from 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. (CQ147302)

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

**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:** TheEEE 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](http://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, and so on, 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:** 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 and all uplink ports of Sx500 and SG500X. (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 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:** 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 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:** 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)

**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:** 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.

**Solution:** There is no workaround.

**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.

### 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](http://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](http://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](http://www.cisco.com/cisco/web/solutions/small_business/products/routers_switches/200_series_switches/index.html)

[www.cisco.com/go/smallbizsupport](http://www.cisco.com/go/smallbizsupport)

---

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Copyright © 2013

78-21436-01