Release Notes for SF250, SG250, SF350, SG350/350X/350XG, SF550X, SG550X/550XG, SX350X, SX550X Series Switches Software Version 2.5.0.79

May 22, 2019

These Release Notes describe the recommended practices and known issues that apply to software version 2.5.0.79 for the products listed in the following table:

Model	Description	Ports
SF250-24	24-Port 10/100 Smart Switch	fa1-fa24, gi1-gi4
SF250-24P	24-Port Gigabit PoE Smart Switch	fa1-fa48, gi1-gi4
SF250-48	48-Port 10/100 Smart Switch	fa1-fa48, gi1-gi4
SF250-48HP	48-Port 10/100 PoE Smart Switch	fa1-fa48, gi1-gi4
SG250-08	8-port Gigabit Smart Switch	gi1-gi8
SG250-08HP	8-port Gigabit PoE Smart Switch	gi1-gi8
SG250-10P	10-Port Gigabit PoE Smart Switch	gi1-gi10
SG250-18	18-port Gigabit Smart Switch	gi1-gi18
SG250-26	26-Port Gigabit Smart Switch	gi1-gi26
SG250-26HP	26-Port Gigabit PoE Smart Switch	gi1-gi26
SG250-26P	26-Port Gigabit PoE Smart Switch	gi1-gi26
SG250-50	50-port Gigabit Smart Switch	gi1-gi50
SG250-50HP	50-port Gigabit PoE Smart Switch	gi1-gi50
SG250-50P	50-Port Gigabit PoE Smart Switch	gi1-gi50

Model	Description	Ports
SG250X-24	24-port Gigabit Smart Switch with 10G Uplinks	gi1-gi24, te1-te4
SG250X-24P	24-port Gigabit PoE Smart Switch with 10G Uplinks	gi1-gi24, te1-te4
SG250X-48	48-port Gigabit Smart Switch with 10G Uplinks	gi1-gi48, te1-te4
SG250X-48P	48-port Gigabit PoE Smart Switch with 10G Uplinks	gi1-gi48, te1-te4
SF350-08	8-Port 10/100 Managed Switch	fa1-fa8
SF350-24	24-Port 10/100 Managed Switch	fa1-fa24, gi1-gi4
SF350-24MP	24-Port 10/100 PoE Managed Switch	fa1-fa24, gi1-gi4
SF350-24P	24-Port 10/100 PoE Managed Switch	fa1-fa24, gi1-gi4
SF350-48	48-Port 10/100 Managed Switch	fa1-fa48, gi1-gi4
SF350-48MP	48-Port 10/100 PoE Managed Switch	fa1-fa48, gi1-gi4
SF350-48P	48-Port 10/100 PoE Managed Switch	fa1-fa48, gi1-gi4
SF352-08	8-Port 10/100 Managed Switch	fa1-fa8, gi1-gi2
SF352-08MP	8-Port 10/100 PoE Managed Switch	fa1-fa8, gi1-gi2
SF352-08P	8-Port 10/100 PoE Managed Switch	fa1-fa8, gi1-gi2
SG350-10	10-Port Gigabit Managed Switch	gi1-gi10
SG350-10MP	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG350-10P	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG350-10SFP	10-Port Gigabit Managed SFP Switch	gi1-gi10
SG350-20	20-Port Gigabit Managed Switch	gi1-gi20
SG350-28	28-Port Gigabit Managed Switch	gi1-gi28
SG350-28MP	28-Port Gigabit PoE Managed Switch	gi1-gi28
SG350-28P	28-Port Gigabit PoE Managed Switch	gi1-gi28
SG350-28SFP	28-Port Gigabit Managed SFP Switch	gi1-gi28

Model	Description	Ports
SG350-52	52-Port Gigabit PoE Managed Switch	gi1-gi52
SG350-52MP	52-Port Gigabit PoE Managed Switch	gi1-gi52
SG350-52P	52-Port Gigabit PoE Managed Switch	gi1-gi52
SG350-8PD	8-Port 2.5G PoE Managed Switch	gi1-gi6, tw7-tw8, te1-te2
SG350X-12PMV	12-port 5G POE Stackable Managed Switch	fi1-fi12, xg1-xg4
SG350X-24	24-Port Gigabit Stackable Managed Switch	gi1-gi24, te1-te4
SG350X-24PV	24-port 5G POE Stackable Managed Switch	gi1-gi8, gi13-gi20, fi9-fi12, fi21-fi24, xg1-xg4
SG350X-24MP	24-Port Gigabit PoE Stackable Managed Switch	gi1-gi24, te1-te4
SG350X-24P	24-Port Gigabit PoE Stackable Managed Switch	gi1-gi24, te1-te4
SG350X-24PD	24-Port 2.5G PoE Stackable Managed Switch	gi1-gi10, gi13-gi22, tw11-tw12, tw23-tw24, te1-te4
SG350X-48	48-Port Gigabit Stackable Managed Switch	gi1-gi48, te1-te4
SG350X-48MP	48-Port Gigabit PoE Stackable Managed Switch	gi1-gi48, te1-te4
SG350X-48P	48-Port Gigabit PoE Stackable Managed Switch	gi1-gi48, te1-te4
SG350X-48PV	48-port 5G POE Stackable Managed Switch	gi1-gi20, gi25-gi44, fi21-fi24, fi45-fi48, xg1-xg4
SG350X-8PMD	8-Port 2.5G PoE Stackable Managed Switch	tw1-tw8, te1-te2
SX350X-08	8-Port 10GBase-T Stackable Managed Switch	te1-te8

Model	Description	Ports
SX350X-12	12-Port 10GBase-T Stackable Managed Switch	te1-te12
SX350X-24	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SX350X-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SX350X-52	52-Port 10GBase-T Stackable Managed Switch	te1-te52
SG355-10P	10-Port Gigabit PoE Managed Switch	gi1-gi10
SF550X-24	24-Port 10/100 Stackable Managed Switch	fa1-fa24, te1-te4
SF550X-24MP	24-Port 10/100 PoE Stackable Managed Switch	fa1-fa24, te1-te4
SF550X-24P	24-Port 10/100 PoE Stackable Managed Switch	fa1-fa24, te1-te4
SF550X-48	48-Port 10/100 Stackable Managed Switch	fa1-fa48, te1-te4
SF550X-48MP	48-Port 10/100 PoE Stackable Managed Switch	fa1-fa48, te1-te4
SF550X-48P	48-Port 10/100 PoE Stackable Managed Switch	fa1-fa48, te1-te4
SG550X-24	24-Port Gigabit Stackable Managed Switch	gi1-gi24, te1-te4
SG550X-24MP	24-Port Gigabit PoE Stackable Managed Switch	gi1-gi24, te1-te4
SG550X-24MPP	24-Port Gigabit PoE Stackable Managed Switch	gi1-gi24, te1-te4
SG550X-24P	24-Port Gigabit PoE Stackable Managed Switch	gi1-gi24, te1-te4
SG550X-48	48-Port Gigabit Stackable Managed Switch	gi1-gi48, te1-te4
SG550X-48MP	48-Port Gigabit PoE Stackable Managed Switch	gi1-gi48, te1-te4

Model	Description	Ports
SG550X-48P	48-Port Gigabit PoE Stackable Managed Switch	gi1-gi48, te1-te4
SX550X-12F	12-Port 10G SFP+ Stackable Managed Switch	te1-te12
SX550X-16FT	16-Port 10G Stackable Managed Switch	te1-te16
SX550X-24	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SX550X-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SX550X-24FT	24-Port 10G Stackable Managed Switch	te1-te24
SX550X-52	52-Port 10GBase-T Stackable Managed Switch	te1-te52
SG350XG-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SG350XG-24T	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SG350XG-2F10	12-Port 10G Stackable Managed Switch	te1-te12
SG350XG-48T	48-Port 10GBase-T Stackable Managed Switch	te1-te48
SG550XG-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SG550XG-24T	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SG550XG-48T	48-Port 10GBase-T Stackable Managed Switch	te1-te48
SG550XG-8F8T	16-Port 10G Stackable Managed Switch	te1-te16

Contents

What's New in this Release

- Mgig 5G interface support—This release adds support for the SG350X-12PMV, SG350X-24PV, and SG350X-48PV switch models, which include multi-gigabit (Mgig) RJ45 copper ports. These switches add support for 5G interfaces, which support 100M/1G/2.5/5Gbps speeds. Mgig ports negotiation is based on 2.5G/5Gbase-T IEEE 802.3bz-2016 and is fully compliant to NBASE-T final spec (version 2.3). The Mgig ports location depends on the switch model.

  As in previous versions, an interface that supports Mgig is named after its maximum port speed. The interface that supports a maximum speed of 5G is named "FiveGigabitEthernet1/0/1," or "fi 1/0/1" for short. As with 2.5G interfaces in previous releases, the numbering of the 5G interfaces is sequential with the 1G interfaces. For example, if the 5G ports were located physically on the seventh and eighth ports, they would be named "tw 1/0/7" and "tw1/0/8."

- Enhanced security—To enhance device management security, this release introduces the following:

  - After you complete the initial connection to a device by logging in with the default user name cisco and the default password cisco, the system requires you to change the user name and password. In previous releases, you were asked to change only the password and could choose to skip the password change process.

NOTE
- Default credentials replacement is also enforced when upgrading from a previous release to this release, if the startup configuration in the previous release does not include level 15 credentials.

-If you disable password complexity, you can configure the user name cisco and the password cisco as your log in credentials. If you save these credentials to startup, you are not prompted to change the credentials.

- The cisco/cisco credentials appear in the device configuration file. In previous releases, the cisco/cisco default credentials did not appear in configuration file.

  - You cannot remove or delete the last privilege level 15 default username and password. This functionality prevents you from reverting (possibly without intention) to the default cisco/cisco credentials. In previous releases, you could remove last level 15 user, and in this case cisco/cisco credentials became active.

  - Deleting device configuration or rebooting a device to factory default restores the default login credentials. In this case, you will need to change the credentials again.

- Runtime defense features include operating system, compiler, and processor features to protect the systems from hacking. The device supports the following related features:

  - X-SPACE—protects the running of unauthorized applications by preventing code from running if it is located in unauthorized memory areas, for example, in a data segment.

  - ASLR—Randomizes the addresses used by the operating system (Linux) for running applications and processes. Each time a process runs, the operating system uses a different address for the process, making it harder for hackers to gain execution permission for their own code.

  - BOSC—Adds protection from buffer overflow (code that tries to access memory that is out of its own memory).

- The following PnP feature support were added to the existing PnP agent behavior:

  - This version supports Cisco Plug and Play connect, which allows full out-of-the-box PNP server discovery that runs over HTTPS. The switch contacts the redirection service using the FQDN devicehelper.cisco.com and then obtains PNP server information from it.

  - Certificate handling (SSL client)/ HTTPS as first choice via DHCP and Cisco Plug and Play connect methods.

  - Downloading of an image and configuration file is protected by MD5 checksum, which is added by the PNP server and validated by the switch.

- The PNP agent and DHCP auto config and image features can now be enabled simultaneously, and both features are enabled by default. If a switch receives a DHCP reply with a PNP agent related option (option 43) and DHCP auto update related options (either options 57 or 125), the switch ignores the PNP agent option information.
- By default, VLAN Mapping Tunneling edge ports drop on ingress L2 PDUs that have the following destination MAC addresses:
  - 01:80:C2:00:00:00-01:80:C2:00:00:FF
  - 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
  - 01:00:0C:CD:CD:D0

  In previous versions, you could not forward frames that had these destination MAC addresses. In this version, you can define a specific port to forward PDUs in any of the following protocols: CDP, LLDP, STP or VPT. (Before the PDUs are forwarded, you must specify a VLAN tag for them.) This functionality allows the forwarding of such untagged frame over the provider network. You also can assign a specific CoS value to such packets and set a threshold rate.
- In addition to STP, RSTP, and MSTP, the device supports PVST+ and RPVST+. PVST+ and /RPVST+ run in separate instances of the 802.1Q STP per VLAN. Rapid PVST runs in a separate instance of the 802.1Q RSTP per VLAN. The device supports up to 126 PVST/RPVST instances.

Downgrade Notes

Boards that are released with the release 2.4.5.x and later use an updated PoE chipset: 6920xM version 0x4a02. In addition to this new chipset version, devices support the following:

- PoE chipset 6920xM version 0x4b42 (used on boards manufactured using software version 2.2.8.4 through 2.4.0.x)
- PoE chipset 6920x version 0x4ac2 (used on boards manufactured using software version 2.1.0.63 through 2.2.7.7)

The PoE chipset version displays as part of the show power inline command output.

Due to the different chipset version support, the following downgrade rules apply:

- Non-PoE devices, and PoE devices that use the original PoE chipset (69208 0x4ac2), follow the same downgrade rules as previous versions: downgrade is supported through the first software version that the device supports

- For Sx250 devices that support PoE chipset 0x4b42, downgrades to software version 2.2.7 or earlier are prevented
- For SG250-10P, SG250-26HP/P, SF250-48HP devices, which support chipset 0x4a02, downgrading from software release 2.4 is prevented
- For SF250-24P, SG250-08HP, SG250-50HP, SG250-50P, SG250X-24P, and SG250X-48P devices, which support chipset 0x4a02, you can downgrade only to version 2.3.5 (the first software version that supports these devices)
- For Sx350 or Sx550 PoE devices that support chipset 0x4a02 or 0x4b42, downgrading software version 2.2.7 or lower is prevented

Known Issues

Open Bugs in Software Version 2.5.0.79

This section lists that bugs that are acknowledged in software version 2.5.0.79.

Table 1 Open Bugs in Software Version 2.5.0.79

Bug ID	Description
CSCvp64736	Symptom: Slave units in stack may reload, due to UDLD operation, under extreme conditions of traffic and perpetual link flapping. Workaround: Disable UDLD on device.
CSCvp64740	Symptom: GUI: The tooltip for suspended interfaces displays incorrect port ID in device view on Dashboard. Workaround: Display issue that has no functional effect; there is no workaround.

Table 1 Open Bugs in Software Version 2.5.0.79 (Continued)

Bug ID	Description
CSCvp64751	Symptom: Stack with master and backup cannot be downgraded to version 2.2.5 (or lower) and then upgraded back to version 2.5. Workaround: Option 1 (use before downgrading is initiated): Delete startup configuration on version 2.5 and then downgrade to version 2.2.5. Option 2 (use if downgrade was already preformed but before upgrading back to 2.5): After downgrading, disconnect the backup unit and then delete the backup unit startup configuration. Reboot the master and backup units, and reconnect the backup unit to the master unit.
CSCvp64768	Symptom: Loopback detection is triggered when PVST/RPVST is enable, even though it should not be. Workaround: Do not enable Loopback detection with PVST/RVPST
CSCvp64778	Symptom: Even if the trunk port is not a member of a VLAN, port RPVST status indicates this VLAN is active. Recommended Action: Display issue, no real affect on functionality.

Open Bugs in Software Version 2.5.0.78

This section lists that bugs that are acknowledged in software version 2.5.0.78.

Table 2 Open Bugs in Software Version 2.5.0.78

Bug ID	Description
CSCvp40302	Symptom: Loopback detection is triggered when PVST/RVPST is enabled, even though it should not be. Workaround: Do not enable Loopback detection with PVST/RVPST.
CSCvp40307	Symptom: Cisco Plug and Play connect—discovery of server IPv4 address fails if both Ipv4 and IPv6 DNS records are received. Workaround: Configure only IPv4 records on the DNS server.

Table 2 Open Bugs in Software Version 2.5.0.78 (Continued)

Bug ID	Description
CSCvp40311	Symptom: The cable-diagnostics tdr always displays “short cable” on 10G ports. Workaround: There is no workaround.
CSCvp40317	Symptom: PSE port connected to specific NICs (not PD device) displays status of “Short” condition. Workaround: There is no workaround.

Resolved Bugs in Software Version 2.5.0.78

This section lists that bugs that are resolved in software version 2.5.0.78.

Table 3 Resolved Bugs in Software Version 2.5.0.78

Bug ID	Description
CSCvn80396	Symptom: sFlow is not working with IPv6, when using default IPv4 address.
CSCvn31587	Symptom: If HTTPS is disabled on a device, you cannot connect to the FindIT Network Probe application from the log in page; relevant for switches on which FindIT Network Probe is enabled. You still can connect to the probe by accessing regular Switch Management from the Login page, and then clicking the FindIT link at the top of the page.
CSCvj32368	Symptom: When using the show green-ethernet command, the display of Power Savings % as a result of short reach setting is not accurate.
CSCvp40263	Symptom: DHCP server will keep offering the first decline address if there is no free address.
CSCvp40272	Symptom: Default ARP timeout keeps 60000 seconds if IP Routing is disabled (but it should be 300 seconds in such case).
CSCvm76475	Symptom: Some MIBs (ifOutDiscards 1.3.6.1.2.1.2.2.1.19) returns NULL value with Cisco Prime.
CSCvn49346	Symptom: DOS: SNMP walking for pacific OID cause device to reboot.

Table 3 Resolved Bugs in Software Version 2.5.0.78 (Continued)

Bug ID	Description
CSCvi71623	Symptom: Pacific Avaya phone LLDP crashes the switch.

Open Bugs in Software Version 2.4.5.71

This section lists that bugs that are acknowledged in software version 2.4.5.71.

Table 4 Open Bugs in Software Version 2.4.5.71

Bug ID	Description
CSCvn31532	Symptom: In some cases, an image upgrade fails when upgrading the image simultaneously to a few devices by using the FindIT Network Probe. Workaround: Wait for the download for each switch to end before upgrading the next switch.
CSCvn31587	Symptom: If HTTPS is disabled on a device, you cannot connect to the FindIT Network Probe application from the log in page; relevant for switches on which FindIT Network Probe is enabled. You still can connect to the probe by accessing regular Switch Management from the Login page, and then clicking the FindIT link at the top of the page. Workaround: Enable HTTPS. This bug is resolved in software version 2.5.0.79.
CSCvn31596	Symptom: FindIT Network Manager fails to cross-launch to a switch on which HTTPS is disabled. Workaround: Enable HTTPS.
CSCvn31554	Symptom: When changing a device IP address from a DHCP to a static IP address, Bonjour broadcasts sent by the switch may contain old IP address information. A new device IP address with a short netmask (less than 20 bits) will not be updated on FindIT Network Probe. Workaround: Reboot the device with the changed IP address.

Resolved Bugs in Software Version 2.4.5.71

This section lists that bugs that are resolved in software version 2.4.5.71.

Table 5 Resolved Bugs in Software Version 2.4.5.71

Bug ID	Description
CSCvj32448	Symptom: In some cases, a fiber link flaps when connecting a SFP MGBLX1 and a 40km fiber cable to some SFP ports. Eventually the link may go down due to link flap prevention.
CSCvj32432	Symptom: Sx550x in hybrid stack mode supports 2,000 Layer 2 Multicast entries (should support 4,000).
CSCvg69635/ CSCvb96602	Symptom: A device sometimes reboots when OOB interface is connected to network with the error message "%2SWPORT-F-Failed2ConvertPort: SW2C_port_get_customer - failed to validate ifIndex -1 relativeIf -1."
CSCvj23510	Symptom: VLAN membership on a trunk mode port is removed if the port native VLAN is not VLAN 1, the port is not a member of all VLANs, and configuration is downloaded and then copied back to the startup configuration.
CSCvk06454	Symptom: Device supports TLS_RSA_WITH_SEED_CBC_SHA weak Cipher suite.
CSCvm20300	Symptom: Device may reload when receiving certain DNS replies in which the DNS responses requested and received IP type (ipv6/ipv4) do not correlate.
CSCvk75871	Symptom: Copying and pasting multiple CLI commands to a console via SSH causes device management to get stuck.
CSCvi65951	Symptom: Packets flood on port-channel (LAG) when the MAC table timeout counter reaches twice its aging time.

Open Bugs in Software Version 2.4.0.94 and 2.4.0.91

This section lists that bugs that are acknowledged in software version 2.4.0.94 and 2.4.0.91.

Table 6 Open Bugs in Software Version 2.4.0.94 and 2.4.0.91

Bug ID	Description
CSCvj32368	Symptom: When using the show green-ethernet command, the display of Power Savings % as a result of short reach setting is not accurate. Workaround: There is no workaround. This bug is resolved in software version 2.5.0.79.
CSCvj32379	Symptom: On some SKUs, fan RPM (Rounds Per Minutes) is displayed as "0" when issuing the show fans system CLI command. Fan functionality is not affected. Workaround: There is no workaround.
CSCvj32418	Symptom: In rare scenarios (adding 700 certain IPv6 routes), hardware routing is disabled even though the resource table is not full. Workaround: Configure fewer or different IPv6 routes. If the issue still occurs, reduce some routes that are not needed and reactivate hardware based routing.
CSCvj32432	Symptom: Sx550x in hybrid stack mode supports 2,000 Layer 2 Multicast entries (should support 4,000). Workaround: Use native mode if possible. This bug is resolved in software version 2.4.5.71.
CSCvj32442	Symptom: The Show inventory command displays wrong information or format of PID and vid = "information not available" for the following SFPs: MFEFX1, MFELX1, MFEBX1, MFEBBX1, MFEBSX1, MFELH1, MFELX1 and MGBT1. This issue affects the display and has no functional effect. Workaround: There is no workaround.
CSCvj32448	Symptom: In some cases, a fiber link flaps when connecting a SFP MGBLX1 and a 40km fiber cable to some SFP ports. Eventually the link may go down due to link flap prevention. Workaround: There is no workaround. This bug is resolved in software version 2.4.5.71.

Table 6 Open Bugs in Software Version 2.4.0.94 and 2.4.0.91 (Continued)

Bug ID	Description
CSCvj32452	Symptom: As of 2.4.0.x, TCP or UDP port range option is not supported in IPv6 ACL and you must use specific ports in ACE configuration. Workaround: After upgrading to 2.4.0.x, ACEs with range configuration are removed from ACL and you must reconfigure specific ports of IPv6 ACL.

Open Bugs in Software Version 2.3.5.63

This section lists that bugs that are acknowledged in software version 2.3.5.63.

Table 7 Open Bugs in Software Version 2.3.5.63

Bug ID	Description
CSCvf88706	Symptom: When connecting an additional unit to an existing stack of 3 units, PoE info for unit 1 is not displayed in CLI or GUI. Workaround: Reboot the stack. This bug is resolved in software version 2.4.0.91.
CSCvf88738	Symptom: Port is suspended (shutdown) when unbinding a specific ACL from port under traffic if the ACL includes a deny ACE with a “disable-port” option. Workaround: shutdown then no shutdown the port to recover. This bug is resolved in software version 2.4.0.91.
CSCvf88746	Symptom: SNA connection to switch is disconnected following switch reboot after upgrade of switch to a new firmware version. Workaround: Refresh browser to reconnect to switch.

Table 7 Open Bugs in Software Version 2.3.5.63 (Continued)

Bug ID	Description
CSCvf88761	Symptom: Enable Ipv6 routing first then configure an Ipv6 6to4 tunnel, tunnel status is “not present.” Workaround: Disable then enable Ipv6 routing or configure the tunnel first then enable Ipv6 routing. This bug is resolved in software version 2.4.0.91.
CSCvf88777	Symptom: SSH connection is slow when connecting from one switch (SSH client) to another switch (SSH server) Workaround: There is no workaround. This bug is resolved in software version 2.4.0.91.
CSCvf88810	Symptom: Non-combo SFP ports will not support 100M SFP module. Workaround: There is no workaround.

Open Bugs in Software Version 2.3.0.130

This section lists that bugs that are acknowledged in software version 2.3.0.130.

Table 8 Open Bugs in Software Version 2.3.0.130

Bug ID	Description
CSCve55065	Symptom: 6to4 tunnel traffic is not forwarded in line rate when the tunnel outgoing port is trunk or general tagged. Workaround: Configure tunnel outgoing port as access or no switch port. This bug is resolved in software version 2.4.0.91.
CSCve55069	Symptom: Some functions in the web GUI not response when using the Apple Safari browser: reboot button, logout, Stop button of Locate Device. Workaround: Use the Google Chrome, Mozilla Firefox, or Microsoft Edge browser.

Table 8 Open Bugs in Software Version 2.3.0.130 (Continued)

Bug ID	Description
CSCve55070	Symptom: When a PoE port is connected to a neighbor that is not a PD, the invalid signature counter keeps increasing. Workaround: This behavior is expected behavior due to the detection process when a non-PD devices is connected to a port.
CSCve55072	Symptom: When defining a time range for a PoE operation and the time range does not include the hour 00:00 as the active time, the PoE consumption values for hours, days and weeks show 0 even if there is a consumption during the displayed period (minutes display correct values). Workaround: There is no workaround. This bug is resolved in software version 2.4.0.91.
CSCve55074	Symptom: In some cases, If the unit-ID setting of a unit in a stack is changed from set ID to auto unit ID, the device does not join the stack after reload. Workaround: Do not change unit ID settings on a unit already in a stack. If the issue happens, disconnect and then reconnect the “stuck” unit from the power source to re-add it to the stack. This bug is resolved in software version 2.3.5.63.
CSCve55078	Symptom: Egress traffic shaping on XG device uplink interfaces limits traffic to 80 Kbps, even if you configured a lower rate. Workaround: Use an egress shaping value higher than 80 Kbps. This bug is resolved in software version 2.4.0.91.
CSCve55081/ CSCve55217	Symptom: On some devices and on certain ports when no cable is connected or cable length is very short, running Cable test via the “test cable-diagnostics tdr” command may provide unpredictable results. Workaround: There is no workaround
CSCve55082	Symptom: If a Cisco 28/29xx terminal server is connected to slave units and “exec” is configured on line, when issuing a reboot command (from master) slave unit reboot may be suspended. Workaround: To prevent this issue, configure “no exec” on line of terminal server before rebooting the stack.

Table 8 Open Bugs in Software Version 2.3.0.130 (Continued)

Bug ID	Description
CSCve55087	Symptom: After a unit switchover from backup to master, the USB interface does not recognize an inserted flash stick (disk on key) Workaround: Reload the unit. This bug is resolved in software version 2.3.5.63.
CSCve55090	Symptom: SNA—when configuring duplex and speed settings for multiple interfaces at the same time, the web page needs to be refreshed to view updated setting. Workaround: Refresh web page
CSCve55094	Symptom: Queue statistics: packet size is calculated based on the packet size on ingress, although statistics are egress statistics. Workaround: There is no workaround.
CSCve55102	Symptom: PoE: In rare cases, the voltage display for ports connected to PD, is lower than actual voltage. Workaround: There is no workaround.
CSCve55112	Symptom: Config migration: when converting a configuration file from a Sx200/Sx300/Sx500 PoE device to a Sx250/Sx350/Sx550 non-PoE device, the following command includes PoE parameter and loading of the file to the destination device fails: “lldp med enable network-policy poe-pse inventory.” Workaround: Manually remove the items related to PoE.
CSCve55117	Symptom: Config migration tool: When converting large files (more than 10,000 lines), the browser may respond slowly or crash. Workaround: There is no workaround.
CSCve55188	Symptom: Web browser can hang due to lack of RAM because SNA does not release RAM correctly when left open for a long time, such as overnight. Workaround: There is no workaround.

Table 8 Open Bugs in Software Version 2.3.0.130 (Continued)

Bug ID	Description
CSCve55203	Symptom: SNA: When selecting multiple devices on which to upgrade firmware and choosing the reboot devices after download option, success indication is provided before the operation completes on all devices. Workaround: There is no workaround.
CSCve55206	Symptom: On XG devices with less than 48 ports, queue statistics from the “show queue statistics” command may show wrong information regarding the number of packets and bytes. Workaround: There is no workaround.
CSCve60999	Symptom: In some cases, a unit may not rejoin a stack after a master switchover (from original master to backup) or when the unit is disconnected and then reconnected to stack. Workaround: Disconnect and then reconnect the “stuck” unit from the power source to re-add it to the stack. This bug is resolved in software version 2.3.5.63.

Open Bugs in Software Version 2.2.8.04

This section lists that bugs that are acknowledged in software version 2.2.8.04.

Table 9 Open Bugs in Software Version 2.2.8.04

Bug ID	Description
CSCvc73697	Symptom: Learned voice VLAN greater than 1024 flush existing VLAN. Workaround: There is no workaround. This bug is resolved in software version 2.3.0.130.

Open Bugs in Software Version 2.2.7.07

There are no new open bugs in software version 2.2.7.07.

Open Bugs in Software Version 2.2.5.68

This section lists that bugs that are acknowledged in software version 2.2.5.68.

Table 10 Open Bugs in Software Version 2.2.5.68

Bug ID	Description
CSCva97565	Symptom: The command “delete sna storage file-name” is missing from the system management chapter of the CLI guide.This command allows the deletion of SNA settings that are saved for a specific user (specified in “file-name” parameter). Workaround: There is no workaround. This bug is resolved in software version 2.2.5.68.
CSCva97578	Symptom: SNA—In rare situations if SNA display is not touched for many hours, the SNA topology display is out of sync. Workaround: Refresh the SNA display.
CSCva97583	Symptom: SNA—In some cases, if a device is preconfigured (via CLI or web) with 802.1x/RADIUS configurations, display/configuration via DAC may fail. Workaround: Remove all manual DAC related settings (802.1x/ RADIUS) from the device before using the DAC feature. This bug is resolved in software version 2.3.0.130.
CSCva97586	Symptom: RSPAN—If traffic is simultaneously forwarded to a destination port due to a mirror operation and another operation (such as regular forwarding), not all traffic is mirrored to the RSPAN destination port Workaround: There is no workaround.

Table 10 Open Bugs in Software Version 2.2.5.68 (Continued)

Bug ID	Description
CSCva97588	Symptom: SNA—When logging in to a device with an IPv6 address using Win10 Edge, cannot view network topology. Workaround: Use an IPv4 address or other browsers to connect. This bug is resolved in software version 2.3.0.130.
CSCva97591	Symptom: SNA—If devices have different times, selecting any statistics in "Connection Explorer" with interfaces selected for devices with different clock times shows incorrect graphs. Workaround: Make sure that all devices have synchronized clocks (for example, via SNTP).
CSCva97601	Symptom: Cannot upgrade firmware and configuration file from an SNA device to devices with version V2.1 or lower. Workaround: Download of firmware to versions earlier than 2.2 is not supported.
CSCva97603	Symptom: If the last physical interface in a VLAN is set to L3 mode and then back to L2 mode, the VLAN status stays down. Workaround: Perform a shutdown/no shutdown on the physical interface. This bug is resolved in software version 2.4.0.91
CSCva97605	Symptom: Upgrading boards running version 2.2.0.x to version 2.2.5.x is not possible via XMODEM. Workaround: Use TFTP for upgrading from version 2.2.0.x to version 2.2.5.x.

Open Bugs in Software Version 2.2.0.63

This section lists that bugs that are acknowledged in software version 2.2.0.63.

Table 11 Open Bugs in Software Version 2.2.0.63

Bug ID	Description
CSCuy97777	Symptom: After reload, the actual spanning tree cost of port-channel is different with running-config. Workaround: There is no workaround. This bug is resolved in software version 2.2.5.
CSCuy97791	Symptom: When STP cost path is equal, Port channel is always selected as root port even if it has a higher priority value. Workaround: STP still functions properly and no loops are created. If needed, use cost setting to change the root port. This bug is resolved in software version 2.2.5.
CSCuy97837	Symptom: On dashboard, the port rx Traffic Error indication shows in red even though the interface counter and rmon statistics of proper ports were cleared. Workaround: There is no workaround. This bug is resolved in software version 2.2.5.
CSCuz01765	Symptom: Some revisions of the Cisco IP Phone 7960 cannot be powered up on switch 60W ports. Workaround: This issue occurs due to a short between phone pins. Connect phone to af/at ports or use Cat 3 cable (2 pairs) to connect a phone to a 60W port.
CSCuy97915	Symptom: Cannot change XG port setting to “disable negotiation” and set speed at the same time via the GUI. Workaround: First disable negotiation and click Apply, then change speed and click Apply.
CSCuy97943	Symptom: In some cases, master unit reloads if stack unit type is changed from fixed to auto. Workaround: Occurs only if stack units are reloaded twice. Stack stabilizes following master reload. This bug is resolved in software version 2.2.5.

Table 11 Open Bugs in Software Version 2.2.0.63 (Continued)

Bug ID	Description
CSCuy97946	Symptom: DHCPv6 relay does not work if destination is set to tunnel interface. Workaround: Use IPv6 Global destination address as DHCPv6 destination.
CSCuy97999	Symptom: When using web based authentication and device DHCP server, unauthenticated station IP address is not expired after station is sent DHCP release. Workaround: Wait until the IP address expires after full lease expiration.
CSCuz45730	Symptom: When negotiating 60W PoE with Cisco PD switches, Cisco PoE-PSE switches sometimes are not able to provide 60W and provide 30W only. Workaround: Connect PD switch to PSE switch before PSE switch boot up. Or disconnect then connect PD switch when issue happens. Or use static 60 watt. This bug is resolved in software version 2.2.5.

Open Bugs in Software Version 2.1.0

This section lists that bugs that are acknowledged in software version 2.5.0.79.

Table 12 Open Bugs in Software Version 2.1.0

Bug ID	Description
CSCux77649	Symptom: When connecting a switch to a Cisco Catalyst compact UPOE PD device, LLDP may not negotiate power on AT / AF ports. Workaround: Use CDP to negotiate. This bug is resolved in software version 2.2.0.

Table 12 Open Bugs in Software Version 2.1.0 (Continued)

Bug ID	Description
CSCux77651	Symptom: When applying policer on ingress interface and sending traffic with multiple priority may result in dropping of higher priority traffic on lower speed egress ports. Workaround: There is no workaround.
CSCux77654	Symptom: Egress ACL cannot be applied to and interface if ACE includes TCP/UDP port range as a parameter. Symptom: Apply required TCP/UDP ports as individual ports in ACL, or apply a range as ingress ACL on relevant interfaces. This bug is resolved in software version 2.2.5.
CSCux77675	Symptom: Aggregate policer QoS statistic always display a value of 0 for both in and out of profile counters. Workaround: There is no workaround. This bug is resolved in software version 2.2.5.
CSCux89410	Symptom: PVID is enabled on an interface when membership type is set to forbidden via the GUI. Interface functionality is not affected. The port still blocks traffic for the relevant VLAN. Workaround: There is no workaround. This bug is resolved in software version 2.2.0.
CSCux89413	Symptom: Auto SmartMacro—In some cases, the interface is set to BPDU guard erri-disable state after replacing the device connected to the interface from a phone/desktop to switch. Workaround: Either disable persistent setting on the interface, or, after the issue occurs, remove the desktop/phone macro from the interface, reactivate the port, and then connect the switch to the interface.
CSCux89418	Symptom: When connecting Sx350P as PD to Sx300P/Sx500P as PSE, Sx350P reboots when disconnecting AC power. After rebooting, Sx350P powers up and functions as expected. Workaround: There is no workaround.

Table 12 Open Bugs in Software Version 2.1.0 (Continued)

Bug ID	Description
CSCux89582	Symptom: Interface is suspended (down) when connecting a copper SFP (MGBT1/GLC-T SFP) with no cable. This issue happens when inserting uplink GE ports (for example, gi3 or gi4) of Sx350/Sx250 or to XG network ports. Workaround: To prevent interface suspension, insert the cable to SFP before inserting SFP to port. If port is already in suspended state, insert the cable into SFP and then activate the suspended port, and the port moves to up state.
CSCux89585	Symptom: If CDP and LLDP are both enabled on a port, disabling one of them may cause the remaining protocol PoE negotiation to fail. Workaround: Do not enable both CDP and LLDP power negotiation at the same time. If the issue occurs, disconnect and then reconnect cable to PD. This bug is resolved in software version 2.3.0.130.
CSCux89597	Symptom: In port limit mode, the default admin power limit value for all types of ports (AF, AT, and 60W PoE) is 30 watts. Workaround: Manually set a limit of 60 watts if needed.
CSCux89611	Symptom: Power negotiation for 60W PoE via LLDP may take up to 1 minute to complete. Symptom: There is no workaround.
CSCux89626	Symptom: When connecting 60W PD to switch, in some cases power indication on switch is higher than 60W. This bug is a display issue. Actual PD consumption is 60W Workaround: There is no workaround.

Open Bugs in Software Version 2.0.0

This section lists that bugs that are acknowledged in software version 2.0.0.

Table 13 Open Bugs in Software Version 2.0.0

Bug ID	Description
CSCuq03628	Symptom: An ISATAP client sends RS packets only when the tunnel interface is disabled and then enabled. Workaround: As long as the tunnel endpoints are both SG350XG/SG550XG, the tunnel works. In mixed devices applications, manually disable and enable the tunnel interface.
CSCur86883	Symptom: When using the web-based configuration interface to set up queue scheduling, you may have a lengthy response time if the system includes a stack of four or more units. Workaround: After about one minute, the web-based configuration interface becomes responsive again, and the setting takes effect. Use the command line interface (CLI) commands for a quicker response time
CSCuu60952	Symptom: When changing an ACE action using the configuration interface, (for example, from deny to shutdown) ACE may be removed from the ACL. Workaround: Reconfigure the ACE, or use the CLI to remove the ACE and then configure it with the new action.
CSCuu60958	Symptom: When configuring a MAC ACE using the web-based configuration interface, creation of new ACE may fail with an error message of “Entry Already Exists,” even though it does not exist. Workaround: Configure the ACE again and it will be accepted, or use the CLI to configure the ACE.
CSCuu60983	Symptom: If VRRP is enabled on a device, DCHP relay using Option 82 fails. Workaround: If VRRP is enabled on device, use DHCP relay without activating Option 82.
CSCuu60986	Symptom: When enabling flow control on the LAG using the user interface, the port LEDs will not light even if link is up. Workaround: This bug is a LED display issue. The functions work as expected. If needed, enable flow control using the command line interface. This bug is resolved in software version 2.2.0.

Table 13 Open Bugs in Software Version 2.0.0 (Continued)

Bug ID	Description
CSCuu60989 CSCuu61046	Symptom: Enabling an 802.1X guest VLAN or a Voice VLAN on a port is forbidden, if the port is a static member of the VLAN and it is in switchport mode (including inactive modes). Workaround: Change the port VLAN membership that use switchport modes so that the port is not a static member in the desired VLAN. NOTE In switchport mode Trunk, the port is a member of all the VLANs by default. Remove the membership in the desired VLANs, or in all VLANs, prior to configuring the 802.1X guest VLAN or the Voice VLAN. This bug is resolved in software version 2.2.5.
CSCuu61008	Symptom: Agreed Auto Voice VLAN cannot be defined as a primary VLAN, even after the voice VLAN is disabled. Workaround: There is no workaround.
CSCuu61061	Symptom: If short reach is enabled on a port, the cable length test using a Cat6a cable fails. Workaround: Disable short reach when running the cable length test on an interface. This bug is resolved in software version 2.2.5.
CSCuu61080	Symptom: DHCP router option (Option 3) is sent by the switch DHCP server, even if the option is not configured for this pool. Workaround: There is no workaround. This bug is resolved in software version 2.2.0.
CSCuu61084	Symptom: IPv6 Routes always display a metric value of “0. Workaround: This bug is a display issue. The correct metric is used for IPv6 L3 forwarding decisions. This bug is resolved in software version 2.2.5.
CSCuu61088	Symptom: The show qos interface command displays info for interfaces that are not present. Workaround: This bug is a display issue only.

Table 13 Open Bugs in Software Version 2.0.0 (Continued)

Bug ID	Description
CSCuu61100	Symptom: Link partner shows that the link is up, even if the device interface is administratively shut down. Workaround: This bug is a display issue. The link is actually down and does not forward traffic.
CSCuu61125	Symptom: The show VLAN command, for VLAN 1, shows non-present interfaces (port and stack units). Workaround: This bug is a display issue only.
CSCuu65516	Symptom: If a language file fails to download (for example, due to a network problem), your Internet browser may display “incomplete/ error information.” Workaround: Delete your browser cookies and try again. The device can still be managed using Telnet.
CSCuu65557	Symptom: If the management session is using the device’s IPv6 address, and this is a secure session (HTTPS), the device cannot be managed using the Safari browser. Workaround: Either use a different browser (such as Internet Explorer) or set up an insecure session (HTTP).
CSCuu65577	Symptom: When using the web-based configuration interface to set a new keychain for RIP, include an accept-lifetime. If you don’t include an accept-lifetime, the configuration doesn't take effect. Workaround: Use a CLI to enter the keychain, or on the user interface, enter both an accept lifetime and a send lifetime.
CSCuu65593	Symptom: On fiber-only ports, negotiation is always enabled; however, the show command displays negotiation as disabled. If the link partner’s negotiation is disabled, the link might not come up. Workaround: Verify that the link partner’s negotiation is enabled.
CSCuu65595	Symptom: MLD Snooping mode on IP v6 inter faces is always (*, G), even if you set the mode to (S, G). Workaround: There is no workaround

Where to Find Support

For current support information, visit the following URLs:

www.cisco.com/c/en/us/support/switches/550x-series-stackable-managed-switches/tsd-products-support-series-home.html

www.cisco.com/c/en/us/support/switches/350x-series-stackable-managed-switches/tsd-products-support-series-home.html

www.cisco.com/c/en/us/support/switches/350-series-managed-switches/tsd-products-support-series-home.html

www.cisco.com/c/en/us/support/switches/250-series-smart-switches/tsd-products-support-series-home.html

www.cisco.com/go/smallbizsupport