Release Notes for SF250, SG250, SF350, SG350, SG350XG, and SG550XG Series Switches Software Version 2.1.0

April 2016

These Release Notes describe the recommended practices and known issues that apply to software version 2.1.0 for the products listed in the following table

Model	Description	Ports
SF250-48	SF250-48 48-Port 10/100 Smart Switch	fa1-fa48, gi1-gi4
SF250-48HP	SF250-48HP 48-Port 10/100 PoE Smart Switch	fa1-fa48, gi1-gi4
SG250-10P	SG250-10P 10-Port Gigabit PoE Smart Switch	gi1-gi10
SG250-26	SG250-26 26-Port Gigabit Smart Switch	gi1-gi26
SG250-26HP	SG250-26HP 26-Port Gigabit PoE Smart Switch	gi1-gi26
SG250-26P	SG250-26P 26-Port Gigabit PoE Smart Switch	gi1-gi26
SF350-48	SF350-48 48-Port 10/100 Managed Switch	fa1-fa48, gi1-gi4
SF350-48P	SF350-48P 48-Port 10/100 PoE Managed Switch	fa1-fa48, gi1-gi4

Model	Description	Ports
SF350-48MP	SF350-48MP 48-Port 10/100 PoE Managed Switch	fa1-fa48, gi1-gi4
SG350-10	10-Port Gigabit Managed Switch	gi1-gi10
SG350-10P	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG355-10P	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG350-10MP	10-Port Gigabit PoE Managed Switch	gi1-gi10
SG350-28	28-Port Gigabit Managed Switch	gi1-gi28
SG350-28P	28-Port Gigabit PoE Managed Switch	gi1-gi28
SG350-28MP	28-Port Gigabit PoE Managed Switch	gi1-gi28
SG550XG-8F8T	16-Port 10G Stackable Managed Switch	te1-te16
SG550XG-24T	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SG550XG-48T	48-Port 10GBase-T Stackable Managed Switch	te1-te48
SG550XG-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SG350XG-24F	24-Port 10G SFP+ Stackable Managed Switch	te1-te24
SG350XG-24T	24-Port 10GBase-T Stackable Managed Switch	te1-te24
SG350XG-48T	48-Port 10GBase-T Stackable Managed Switch	te1-te48
SG350XG-2F10	12-Port 10G Stackable Managed Switch	te1-te12

Contents

What's New in this Release

- IP subnet based VLAN—VLAN classification of an untagged frame on ingress interface based on the frame source IP address or subnet. IP subnet classification has lower priority than MAC based VLAN but higher priority than protocol based VLAN.
- Switched Port Analyzer (SPAN)—Allows you to define multiple mirroring sessions, each of which defines a single target and multiple source interfaces. The target port can be defined as a network port, meaning it receives both monitored and regular network traffic in parallel. SPAN commands replace exiting port monitor function and commands.
- Policy based flow mirroring—Using policy map to mirror a specific traffic flow to an analyzer port based on the class map classification, and using a SPAN session.
- Egress ACL/policy—Allows configuration of ACL and Policy Maps on an egress interface (in addition to the existing behavior, which allows the configuration on an ingress interface).
- 2 Rate 3 Color (2R3C) policer—Allows configuration, as part of a policer, of two separate bandwidth limitation levels (and bursts): committed rate and peak rate. For each traffic limitation, an drop or DSCP remark action can be set for traffic that exceeds the limitations. This configuration creates 3 rate levels (committed, peak and exceeding), which correspond to 3 color levels (green, yellow and red).
- Link-flap prevention—Set an interface that is experiencing multiple link flaps (link down and up events) to the err-disable state, with relevant syslog message to user.

- PoE PD—Specific SKUs support the PoE PD capability on uplink interfaces. These SKUs can be powered via PoE by connecting them to an uplink PoE switch/device (PSE).
- POE 60W PoE—Specific SKUs and ports support POE 60W PoE capability. 60W POE extends the PoE+ standard to double the power per port up to 60 watts. Supporting ports include PSE and PD type ports.
- PoE CDP/LLDP negotiation—The ability of PD and PSE to negotiate the required power level using CDP or LLDP protocols. This ability is supported on switch PD and PSE ports functionality
- SLFOW v5—An embedded sampling technology (based on RFC 3176) that provides the ability to continuously monitor traffic flows and counters on some or all interfaces simultaneously. The sFlow monitoring system consists of the sFlow Agent (embedded in the device) and a central data collector, or sFlow Analyzer.
- CLI Output modifier—Filter the display of the output of CLI show commands based on specific text, which is included or not included in the lines of the show command output.
- Dashboard/Wizard—ACL Wizard and following dashboards: PoE utilization, Traffic error, and Port utilization.
- Save icon functionality enhancement—When clicking the save icon, the running configuration is copied to the startup configuration without changing the page to the Download/Backup Configuration/Log page, and a progress indicator is displayed,
- Syslog Popup—When a new syslog is written to the RAM log file, a notification is displayed in the web GUI. The notification shows the syslog contents and allows you to track log information in real time.
- Show Tech-Support in web-GUI—Allows you to view in the GUI the output of the show tech-support CLI command, and copy-past this output to your PC.
- Counter history and graph—Table (CLI) and graphical display (GUI) of interface counter statistics history, port utilization, and counters ingress unicast/multicast/broadcast frames and total bytes. You can define the time span for the graph.
- GUI page search—GUI search tool, which allows locating pages that include words or phrases specified in the search window. This feature is useful for locating the page or pages that included certain settings that you require.

Issues Resolved

No issues resolved in this release.

Known Issues

Open Bugs in Software Version 2.1.0

This section lists that bugs that are acknowledged in software version 2.1.0:

Table 1 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.
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.
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.

Table 1 Open Bugs in Software Version 2.1.0 (Continued)

Bug ID	Description
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.
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.
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.

Table 1 Open Bugs in Software Version 2.1.0 (Continued)

Bug ID	Description
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 2 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

Table 2 Open Bugs in Software Version 2.0.0 (Continued)

Bug ID	Description
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.
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.
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.

Table 2 Open Bugs in Software Version 2.0.0 (Continued)

Bug ID	Description
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.
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.
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.
CSCuu61088	**Symptom:** The **show qos interface** command displays info for interfaces that are not present. **Workaround:** This bug is a display issue only.
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.

Table 2 Open Bugs in Software Version 2.0.0 (Continued)

Bug ID	Description
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