ıllıllı
CISCO ™

Release Notes for 200 and 300 Series Switches Software Version 1.1

June 2011

These Release Notes describe the recommended practices and known issues that apply to the Version 1.1 software for the following products:

Model	Description	Ports
SF 200-24	24-Port 10/100 Smart Switch	e1-e24, g1-g2
SF 200-24P	24-Port 10/100 PoE Smart Switch	e1-e24, g1-g2
SF 200-48	48-Port 10/100 Smart Switch	e1-e48, g1-g2
SF 200-48P	48-Port 10/100 PoE Smart Switch	e1-e48, g1-g2
SG 200-18	18-port Gigabit Smart Switch	g1-g18
SG 200-26	26-port Gigabit Smart Switch	g1-g26
SG 200-26P	6-port Gigabit PoE Smart Switch	g1-g26
SG 200-50	50-port Gigabit Smart Switch	g1-g50
SG 200-5P	50-port Gigabit PoE Smart Switch	g1-g50
SG 300-10	10-port Gigabit Managed Switch	g1-g10
SG 300-10MP	10-port Gigabit PoE Managed Switch	g1-g10
SG 300-10P	10-port Gigabit PoE Managed Switch	g1-g10
SG 300-20	20-port Gigabit Managed Switch	g1-g20
SG 300-28	28-port Gigabit Managed Switch	g1-g28
SG 300-28P	28-port Gigabit PoE Managed Switch	g1-g28

Release Notes

Model	Description	Ports
SG 300-52	52-port Gigabit Managed Switch	g1-g52
SF 300-08	8-port 10/100 Managed Switch	e1-e8
SF 302-08	8-port 10/100 Managed Switch	e1-e8, g1-g2
SF 302-08MP	8-port 10/100 PoE Managed Switch	e1-e8, g1-g2
SF 302-08P	8-port 10/100 PoE Managed Switch	e1-e8, g1-g2
SF 300-24	24-port 10/100 Managed Switch	e1-e24, g1-g4
SF 300-24P	24-port 10/100 PoE Managed Switch	e1-e24, g1-g4
SF 300-48	48-port 10/100 Managed Switch	e1-e48, g1-g4
SF 300-48P	48-port 10/100 PoE Managed Switch	e1-e48, g1-g4

These caveats apply to:

SW version: 1.1.0.73

Sx300 Boot version HW 1.0: 1.0.0.4

Sx200 Boot version HW 1.0: 1.0.0.1

Sx300 Boot version HW 1.1: 1.1.0.6

Sx200 Boot version HW 1.1: 1.1.0.6

Contents

Hardware Versions

The Release 1.1 firmware runs on two different versions of hardware for the 200 Series Smart Switches, and the 300 Series Managed 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 HW VID=01	8K	128	128
Sx200 in Firmware 1.1 HW VID=01	8K	256	256
Sx200 in Firmware 1.1 HW VID=02	8K	256	256
Sx300 in Firmware 1.0 HW VID=01	8K	256	256
Sx300 in Firmware 1.1 HW VID=01	8K	256	256
Sx300 in Firmware 1.1 HW VID=02	16K	4K	1K

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.

Known Issues When Upgrading

The following issues and possible corrective measures are related to upgrading from release 1.0 to 1.1.

- **Issue 1**: The back-up configuration becomes unusable after upgrading from release 1.0 to release 1.1.
  Workaround: The configuration file can be used by performing the following three steps:

  - Download the backup configuration file via HTTP / TFTP.

  - Delete the corrupted portion (repeated random character) at the end of the file.

  - Upload the configuration back to the switch.

- **Issue 2**: AutoConfig option 66 67—The switch will not reboot after downloading a configuration file from a TFTP server to the startup configuration via Auto Configuration (option 66/67) due to syntax error or configuration file. This is due to the incompatibility between commands from release 1.0 and release 1.1.

- **Issue 3**: Some configurations might fail when upgraded from release 1.0 to release 1.1. The following configuration commands/features might be impacted.

  - The http/https idle time out configuration will be deleted.
    Workaround: Reconfigure the http/https idle timeout.

  - The Advanced QoS configuration such as class maps, policy maps and aggregate policers, will not be applied and gets deleted after the upgrade.
    Workaround: Backup the startup configuration from the switch to a local PC/host before the upgrade, and reconfigure the missing QoS Advanced configuration after upgrading.

  - The access method configuration might have issues due to the incompatibility of `ip http authentication` commands (Bugs133551)
    Workaround: `ip http authentication radius tacacs local` needs to be replaced with `ip http authentication aaa login-authentication radius tacacs local` after upgrade.

  - Creation of users might exhibit a problem due to the incompatibility of username commands.

Workaround: Replace the release 1.1 command for user creation after upgrade. For example:

1.0.0.x—`username cisco password da39a3ee5e6b4b0d3255bfef95601890afd80709 level 15 encrypted`

1.1.0.73—`username cisco password encrypted 59892959e6c8d6d726a97e11c3da0e5c2e856cd5 privilege 15`

- The VLAN database will be duplicated twice in the configuration file. There is no impact on the switch functionality.

- **Issue 4**: Release 1.0 second language file is invalid after upgrading to release 1.1
  Workaround: Download a release 1.1 language file.

Limitations and Restrictions

Problem: SNTP broadcast reception works correctly when enabled through the GUI, but when the configuration is entered into the CLI, the broadcast client does not synchronize correctly. (Bugs00133199)

Solution: When an SNTP client is configured from the CLI, the `clock source` command must be executed after configuring SNTP for the SNTP client to initialize and be running.

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

Solution: There is no workaround.

Problem: Whenever the Short Reach option is checked on a given port, the EEE option is grayed out but EEE LLDP is not. However, when checked and then the apply button is pressed, the correct error message is being displayed. (Bugs00132049)

Solution: When Short Reach mode is going to be used, uncheck both EEE and EEE(LLDP). Check Short Reach mode and do not check the EEE(LLDP) or it will exhibit an error message.

Problem: The EEE operational status should become disabled when Auto Negotiation is disabled. (Bugs00132106)

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. (Bugs00132684)

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

Problem: Copying configuration information from one port to another doesn't copy all the settings:

- On the **Security > Port Security** page, Trap and Trap Frequency fail to copy when port security settings are copied from one interface to other interfaces. (Bugs00132724)

- On the **Vlan Management > Interface Settings** page, the Copy Settings functionality drops the Administrative PVID when copying settings from one port to another. (Bugs00132132)

Solution: Configure the port settings individually instead of all at once.

Problem: When the Mrouter learning mode is changed between "user defined" to "auto" and vice-versa, the IGMP Querier election process doesn't start. (Bugs00132805)

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

Problem: Source specific multicast filtering is not supported on VLAN that has Bonjour/VSDP enabled. (Bugs00131405)

Solution: There is no workaround.

Problem: Configuration of source specific IPv6 multicast groups in forbidden mode performs as expected, but does not reflect on the Web User Interface. (Bugs00132433)

Solution: Verify the group membership from the CLI interface.

Problem: On a PC running windows XP, and using Internet Explorer version 6, some graphics do not show the correct color. (Bugs00133242)

Solution: There is no workaround.

Problem: On a PC running windows XP, and using Firefox version 2.0.0.20, some of the pages in the Web User Interface do not load. (Bugs00133243)

Solution: There is no workaround.

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

Solution: For download and installation please refer the following link:

www.microsoft.com/downloads/details.aspx?FamilyID=993C0BCF-3BCF-4009-BE21-27E85E1857B1&displaylang=en

Problem: Notification Recipients table entry becomes un-editable with an incorrect or missing parameter. (Bugs00133316)

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

Problem: SNMPv3 notification authentication configuration is unrelated to user authentication configuration. (Bugs00133074)

Solution: The user needs to remember the authentication/privacy settings configured for the group of the user and for the user and select the appropriate authentication/privacy setting.

Problem: Usage of hexadecimal key format for specifying authentication keys (SHA or MD5 methods) while configuring an SNMPV3 user is not supported. (Bugs00132885)

Solution: Use the password format instead. If the configuration requires using the key format, use the web user interface.

Problem: The result of cable length test for 100 meters is incorrect. It will show between 110 to 140 meters. (Bugs00132941)

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." (Bugs00130161)

Solution: There is no workaround.

Problem: Proxy ARP functions for subnets sharing the same class based network. It will not work if the subnets in question belong to 2 different class based networks. (Bugs00130163)

Example: ARP proxy forwards requests/responses between subnets 192.168.5.0/ 28 and 192.168.5.32/28 which belong to the same class based network 192.168.5.0. The same principle applies when dealing with class A or B networks.

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. (Bugs00132211)

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. (Bugs00133234)

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

Problem: When a DVA authorized port tries to re-authenticate and RADIUS attributes no longer include VLAN attributes, reauthentication should fail and the port should become unauthorized. This is not happening, and the port does not fail. (Bugs00131469)

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

Problem: Egress rate shaping does not work as expected. Configuring egress shape on Gigabit ports or on Combo ports between 64k to 5000k, will always result in 2 Million Bits. This is resolved with the new hardware release 1.1. It still exists on HW 1.0. It also does not work on SG300-52/52P & SG200-52/52P switches. (Bugs00123397 and Bugs00130715)

Solution: There is no workaround.

Problem: The File Name box on the Download/Backup Firmware/Language page appears enlarged and blue after the file is download. (Bugs00132175)

Solution: Click the reload button while on the page.

Problem: Login fails when using the"+"' character at the end of a Username or Password. (Bugs00132366)

Solution: There is no workaround, avoid using the "+" character.

Problem: When the `clear cdp table` command is executed on the console all the phones are rebooted. The console logs show the voice VLAN goes down then comes back up. (Bugs00132482)

Solution: Avoid using the command.

Problem: SNTP synchronization error messages are not logged when an incorrect MD5 key leads to the loss of synchronization. (Bugs00132636)

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.

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/300_series_switches/index.html

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

www.cisco.com/go/smallbizsupport

OL-25422-01