Release Notes for the Cisco CGS 2520, Cisco IOS Release 12.2(58)SE and Later

Part Number: OL-25033-02
Updated: January 3, 2012

Cisco IOS Release 12.2(58)SE and later runs on the Cisco Connected Grid Switch (CGS) 2520.

Note Cisco IOS Release 12.2(58)SE images for all platforms were removed from Cisco.com because of a severe defect, CSCto62631. The solution for the defect is in Cisco IOS Release 12.2(58)SE1.

These release notes include important information about Cisco IOS Release 12.2(58)SE and later and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

For the complete list of CGS 2520 switch documentation, see the "Related Documentation" section on page 20.

You can download the switch software from this site (registered Cisco.com users with a login password): http://www.cisco.com/cisco/web/download/index.html

Tell Us What You Think

Send your feedback about this document directly to the Connected Grid Documentation Team.

Connected Grid Documentation Feedback Form

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

System Requirements

Hardware Supported

Table 1 Cisco CGS 2520 Hardware Models

Model	Description
Cisco CGS-2520-24TC	24 10/100 Fast Ethernet ports, 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP[1] module slots), and 2 AC- and DC-power-supply module slots.
Cisco CGS-2520-16S-8PC	16 100BASE-FX SFP-module slots; 8 10/100 Fast Ethernet PoE[2] ports, 2 dual-purpose ports (2 10/100/1000BASE-T copper ports and 2 SFP module slots), and 2 AC- and DC-power-supply module slots.

Table 1 Cisco CGS 2520 Hardware Models (continued)

Model	Description
SFP modules[3]	Rugged and Industrial SFP modules • GLC-SX-MM-RGD (rugged SFP) • GLC-LX-SM-RGD (rugged SFP) • GLC-ZX-SM-RGD (rugged SFP) • GLC-FE-100LX-RGD (rugged SFP) • GLC-FE-100FX-RGD (rugged SFP) Commercial SFPs • GLC-BX-D with digital optical monitoring (DOM) support • GLC-BX-U with DOM support • GLC-FE-100LX • GLC-FE-100BX-D • GLC-FE-100BX-U • GLC-FE-100FX • GLC-FE-100EX • GLC-FE-100ZX • CWDM SFP with DOM support Extended Temperature SFP modules • SFP-GE-L with DOM support • SFP-GE-S with DOM support • SFP-GE-Z with DOM support • GLC-EX-SMD with DOM support
SFP module patch cable	CAB-SFP-50CM
Power supply modules	PWR-RGD-AC-DC PWR-RGD-LOW-DC **Note** For power supply module descriptions and supported configurations on switch models, see the hardware installation guide.

1. SFP = small form-factor pluggable.
2. PoE = Power over Ethernet.
3. The maximum operating temperature of the switch varies depending on the type of SFP module that you use. See the *Cisco CGS 2520 Switch Hardware Installation Guide* for more information.

Device Manager System Requirements

The device manager is a web application stored in the switch memory that supports quick configuration. For more information about the device manager, refer to the *Cisco CGS 2520 Getting Started Guide.*

Hardware Requirements

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Windows 2000, XP, Vista, or Windows Server 2003.
- Web browser (Internet Explorer 6.0, 7.0, or Firefox 1.5, 2.0 or later) with JavaScript enabled.

The device manager verifies the browser version when starting a session, and it does not require a plug-in.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the compact flash memory card.

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory. For example, use the **dir flash:** command to display the images in the flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the filenames for this software release.

If you download the IP services image and plan to use Layer 3 functionality, you must use the Switch Database Management (SDM) routing template. To identify the active SDM template, enter the **show sdm prefer** privileged EXEC command. If necessary, enter the **sdm prefer** global configuration command to change the SDM template to a specific template. For example, if the switch uses Layer 3 routing, change the SDM template from the default to the routing template.You will need to reload the switch for the new template to take effect.

Table 3 Cisco IOS Software Image Files

Filename	Description
cgs2520-lanbaselmk9-tar.122-58.SE2.tar	CGS 2520 cryptographic image file and device manager files with Layer 2+ features. This image has the Kerberos and SSH features.
cgs2520-ipserviceslmk9-tar.122-58.SE2.tar	CG 2520 IP services cryptographic image with device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch Using the CLI

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

Note Make sure that the compact flash card is inserted into the switch before downloading the software.

To download software, follow these steps:

Step 1 Use Table 3 on page 5 to identify the file that you want to download.

Step 2 To download the software image file, go to the following URL, and log in to download the appropriate files:
http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.
For more information, see the *Cisco CGS 2520 Software Configuration Guide*.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory*/*image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/image-name.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For additional recovery procedures, see the "Troubleshooting" chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program, as described in the *Cisco CGS 2520 Getting Started Guide*.
- The CLI-based setup program, as described in the *Cisco CGS 2520 Hardware Installation Guide*.
- The DHCP-based autoconfiguration, as described in the *Cisco CGS 2520 Software Configuration Guide*.
- Manually assigning an IP address, as described in the *Cisco CGS 2520 Software Configuration Guide*.

New Software Features

Cisco IOS Release 12.2(58)SE and later does not contain new software features for the Cisco Connected Grid Switch (CGS) 2520.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

These Cisco IOS limitations apply to the CGS 2520:

- Trunking, page 15
- VLAN, page 15

Bidirectional Forwarding Detection (BFD)

- The BFD session with the neighbor flaps when there is close to 100 percent bidirectional line- rate traffic sent through the physical links connecting the neighbors. This happens only on those sessions in which Layer 3 BFD neighboring switches connect through a Layer 2 intermediate switch.

  The workaround is to ensure that there is no 100 percent bidirectional unknown traffic flowing through the intermediate Layer 2 switch in the same links that connect Layer 3 switches. An alternate workaround is to always directly connect the Layer 3 switches when BFD is running. (CSCsu94835)
- When you create a BFD session between two switches and create an ACL that includes the **permit ip any any log-input** access-list configuration command, the BFD session goes down when you attach the ACL to one of the connecting interfaces. When you remove the ACL from the interface, BFD comes back up.

  The workaround is to not use the **permit** ACL entry with the log option on interfaces participating in BFD. (CSCtf31731)

Connectivity Fault Management (CFM)

- When the CFM start delay timer is configured to a small value, the Crosscheck-Up field in the output of the **show ethernet cfm domain** privileged EXEC command and the Mep-Up field in the output of the **show ethernet cfm maintenance-points remote crosscheck** privileged EXEC command might appear as *No* even if the CCM is learned in the remote database.

  This is expected behavior. The workaround is to use the **ethernet cfm mep crosscheck start-delay** command to set the start-delay timer value larger than the continuity-check interval. (CSCtf30542)

Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:
  - When the switch is booted without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)
- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:
  - When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.

  - The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. When the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)

- When dynamic ARP inspection is enabled on a switch, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)

- Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost.

  When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command.

  There is no workaround. (CSCed95822)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked.

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs when a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- When a switch starts, SFP ports can become active before the Cisco IOS software loading process is complete. Packets arriving at these ports before the switch software is completely loaded are lost. This is a hardware limitation when the switch uses small form-factor pluggable (SFP) modules with copper connections.

  The workaround is to use switch ports other than those specified for redundancy and for applications that immediately detect active links. (CSCeh70503)

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse (CSCsh12472):

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)

- When the configuration file is removed from the switch and the switch is rebooted, port status for VLAN 1 and the management port (Fast Ethernet 0) is sometimes reported as *up* and sometimes as *down*, resulting in conflicts. This status depends on when you respond to the reboot query:

  ```
  Would you like to enter the initial configuration dialog?
  ```

  - After a reboot if you wait until the Line Protocol status of VLAN 1 appears on the console before responding, VLAN 1 line status is always shown as *down*. This is the correct state.
  - The problem (VLAN 1 reporting *up*) occurs if you respond to the query before VLAN 1 line status appears on the console.

  The workaround is to wait for approximately 1 minute after rebooting, and until the VLAN 1 interface line status appears on the console before you respond to the query. (CSCsl02680)

- CPU utilization increases when the traffic on a switch is disrupted by an Address Resolution Protocol (ARP) broadcast storm even if broadcast storm control is enabled.

  There is no workaround. (CSCtg31923)

EtherChannel

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

  There is no workaround. (CSCsh12472)

- When an EtherChannel is configured for 802.1ad and a channel member that is up is removed from the EtherChannel, the 802.1ad configuration is removed. However, if the member channel is shut down and then removed from the EtherChannel, the 802.1ad configuration is not removed.

  The workaround is to enter the **no shutdown** interface configuration command on the member channel before removing it from the EtherChannel. (CSCtf77937)

IP

- The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out.

  The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

- When the rate of received DHCP requests exceeds 2000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service (DoS) attack from occurring. (CSCea21674)

IP Service Level Agreements (SLAs)

- When the IP SLAs configured reaction type (configured by entering the **ip sla reaction-configuration** global configuration command) is round-trip time (RTT), an RTT event causes duplicate SNMP traps.

  There is no workaround.

IP Telephony

- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned.

  No workaround is necessary. (CSCea85312)

- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

  The workaround is to enable Power over Ethernet (PoE) and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

Fallback Bridging

- If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group.

  The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)

- Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group.

  The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the **no switchport port-security** interface configuration command. (CSCdz80499)

MAC Addressing

- When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped.

  There is no workaround. (CSCeb67937)

Multicasting

- The switch does not support tunnel interfaces, including DVMRP and PIM tunneling.
- Non-reverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port.

  There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)

- Non-reverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN leaks when the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise.

  The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)

- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port.

  There is no workaround. (CSCdy82818)

- When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN.

  The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means. For example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)

- When an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - When the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - When the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast interface** configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

- When IP routing is disabled and IP multicast routing is enabled, IGMP snooping floods multicast packets to all ports in a VLAN.

  The workaround is to enable IP routing or to disable multicast routing on the switch. You can also use the **ip igmp snooping querier** global configuration command when IP multicast routing is enabled for queries on a multicast router port. (CSCsc02995)

QoS

- When you use the **bandwidth policy-map class** command to configure more than one class in a policy map for Class-based Weighted Fair Queuing (CBWFQ), and the committed information rate (CIR) bandwidth for any of the classes is less than 2 percent of the interface rate, the CBWFQ classes in the policy might not receive the configured CIR bandwidths.

  There is no workaround, but it is unlikely that a CBWFQ class would be configured with such a low CIR bandwidth. (CSCsb98219)

- When several per-port, per-VLAN parent policies are attached to the input of one or more interfaces and a child policy of these parent policies is modified, the parent policies are detached from the interfaces and reattached during the process. Because the modified policy is large, the TCAM entries are being used up, and the attached policies should be removed. However, some of the parent policies are not removed from the interface, and the TCAM entries are cleared. When you save the configuration and reload the switch, the policies are detached, but the TCAM is full, and you cannot attach other policies.

  This error message appears:

  QOSMGR-4-QOS_TCAM_RESOURCE_EXCEED_MAX: Exceeded a maximum of QoS TCAM resources

  The workaround is to manually detach the policy maps from all the interfaces by entering the **no service-policy input** *policy-map-name* interface configuration command on each interface. (CSCsk58435)

REP

- Although you can configure a REP segment without configuring REP edge ports, Cisco recommends that you configure REP edge ports whenever possible because edge ports enable these functions:
  - Selecting the preferred alternate port
  - Configuring VLAN load balancing
  - Configuring topology change notifications (TCNs) toward STP, other REP segments, or an interface
  - Initiating the topology collection process
  - Preemption mechanisms

  You cannot enable these functions on REP segments without edge ports.

- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1000 milliseconds (1 second), the REP link flaps when the BFD interface is shut down and then brought back up.

  The workaround is to use the **rep lsl-age-out timer** interface configuration command to configure the REP LSL age timer for more than 1 second. (CSCsz40613)

- When you configure two or more connected REP segments to send segment topology change notices (STCNs) by entering the **rep stcn segment** *segment-id* interface configuration command on REP interfaces, and segments inject messages simultaneously, an STCN loop occurs, and CPU usage can increase to 99 percent for 1 to 2 minutes before recovering.

  The workaround is to avoid configuring multiple STCNs in connected segments. This is a misconfiguration. (CSCth18662)

Routing

- The switch does not support tunnel interfaces for routed traffic.
- A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported.

  There is no workaround. (CSCea52915)
- A spanning-tree loop might occur when all of these conditions are true:
  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

  The workaround is to change any one of the listed conditions. (CSCed53633)

SPAN and RSPAN

- When system jumbo MTU size is configured on a switch and the egress ports can support jumbo frames, the egress SPAN jumbo frames are not forwarded to the SPAN destination ports.

  There is no workaround. (CSCsj21718)
- Cisco Discovery Protocol (CDP) and Port Aggregation Protocol (PAgP) packets received by network node interfaces (NNIs) from a SPAN source are not sent to the destination interfaces of a local SPAN session.

  The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)
- An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets.

  The workaround for local SPAN is to use the **replicate** option. For a remote SPAN session, there is no workaround. (CSCdy72835)
- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets.

  The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround. (CSCdy81521)
- The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, when the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console

message appears: *Decreased egress SPAN rate.* In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. When fallback bridging and multicast routing are disabled, egress SPAN is not degraded.

There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

- Some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned.

  There is no workaround. (CSCeb23352)

Trunking

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN *X* but is not a member in VLAN Y. If VLAN *Y* is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN *Y* belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN *Y* is sent on the trunk port in VLAN *Y* because the trunk port is forwarding in VLAN *Y*, even though the port has no group membership in VLAN *Y*.

  There is no workaround. (CSCdz42909).

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

  There is no workaround. (CSCec35100).

VLAN

- When the number of VLANs times the number of trunk ports exceeds 13,000 the switch can stop.

  The workaround is to not configure more than the recommended number of VLANs and trunks. (CSCeb31087)

- A CPUHOG message sometimes appears when you configure a private VLAN, and port security is enabled on one or more of the ports affected by the private VLAN configuration.

  There is no workaround. (CSCed71422)

- When you apply a per-VLAN quality of service (QoS), per-port policer policy-map to a VLAN Switched Virtual Interface (SVI), the second-level (child) policy-map in use cannot be re-used by another policy-map.

  The workaround is to define another policy-map name for the second-level policy-map with the same configuration to be used for another policy-map. (CSCef47377)

- When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state.

  The workaround is to configure the burst interval to more than 1 second. (CSCse06827)

- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

Important Notes

Auto-negotiation Configuration in Cisco IOS Release 12.2(28)SE and Higher

When you upgrade the switch software to Cisco IOS release 12.2(28)SE or higher and auto-negotiation is enabled on a Gigabit SFP fiber switch port (the default), but disabled on the link partner port, the switch port interface can show a state of *down/down* while the link partner shows *up/up*. This is expected behavior.

- The workaround is to either enable autonegotiation on the link partner port or enter the **speed nonegotiate** interface command on the SFP port.

Configuring the Device Manager and HTTP Server Interface

We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

From Microsoft Internet Explorer:

1. Choose **Tools** > **Internet Options**.
2. Click **Settings** in the “Temporary Internet files” area.
3. From the Settings window, choose **Automatically**.
4. Click **OK**.
5. Click **OK** to exit the Internet Options window.

The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is disabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

Open Caveats

- CSCtj88307

  When you enter the default interface, switchport, or no switchport interface configuration command on the switch, this message appears: *EMAC phy access error, port 0, retrying.....*

  There is no workaround.

- CSCtg98453

  When you make port security changes on an interface, such as configuring aging time, violations, or aging type, error messages and tracebacks might appear.

  There is no workaround.

- CSCtl32991

  Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue. This does not occur when packets are routed through the switch to another destination.

  There is no workaround.

- CSCtl60247

  When a switch running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. When the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

- CSCtl81217

  When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, when the switch reloads, the interface loses some of the RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.

  There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:

  ip rip authentication mode

  ip rip key-chain

Resolved Caveats

- CSCtl51859

  Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.

  The workaround is to disable IPv6 MLD snooping on the switch.

- CSCtg52770

  When the switch receives more than 1000 IPv6 prefixes from the Border Gateway Protocol (BGP), the CPU utilization increases.

  There is no workaround.

- CSCtg54162

  The switch fails when it adds IPv6 routes to the ternary content addressable memory (TCAM).

  The workaround is to reload the switch by entering the **reload** privileged EXEC command.

- CSCtj03875

  When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.

  There is no workaround.

- CSCtj83964

  On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.

  The workaround is to enter the **clear ip route** privileged EXEC command or reconfigure PIM and SSM after a reload.

- CSCto10165

  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.shtml.

- CSCto62631

  A switch running Cisco IOS Release 12.2(58)SE1 might reload when:

  - SSH version 2 is configured on the switch, and
  - a customized login banner was configured by using the **banner login message** global configuration command.

  Use one of these workarounds:

  - Disable the login banner by entering the **no login banner** command.
  - Disable SSH on the switch.
  - Downgrade to a software version earlier than Cisco IOS Release 12.2(58)SE1.

- CSCtq01926

  When you configure a port to be in a dynamic VLAN by entering the **switchport access vlan dynamic** interface configuration command on it, the switch might reload when it processes ARP requests on the port.

  The workaround is to configure static VLANs for these ports.

Documentation Updates

Corrections for the Regulatory and Compliance Guide

These are updates to the *Regulatory Compliance and Safety Information for the Cisco CGS 2520*:

- The regulatory standards compliance table incorrectly lists the Industrial and Physical Security certifications. These do not apply to the switch.
- The regulatory standards compliance table incorrectly lists Reduction of Hazardous Substances (ROHS) 6. The switch is ROHS 5-compliant.

Related Documentation

http://www.cisco.com/en/US/products/ps10978/tsd_products_support_series_home.html

- *Cisco CGS 2520 Software Configuration Guide*
- *Cisco CGS 2520 Command Reference*
- *Cisco CGS 2520 System Message Guide*
- *Cisco CGS 2520 Hardware Installation Guide*
- *Cisco CGS 2520 Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, Brazilian Portuguese, and Spanish
- *Installation Notes for the Power Supply Modules for the Cisco CGS 2520*
- *Regulatory Compliance and Safety Information for the Cisco CGS 2520*

SFP module installation notes:
http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*

Compatibility matrix documents:
http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- Cisco Small Form-Factor Pluggable Modules Compatibility Matrix
- Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.