Release Notes for the Cisco Catalyst Blade Switch 3130 and 3032 for Dell, Cisco IOS Release 12.2(58)SE1

Revised December 22, 2011

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.

Cisco IOS Release 12.2(58)SE1 runs on the Cisco Catalyst Blade Switch 3130 and 3032 for Dell switches. The Cisco Catalyst Blade Switch 3130 supports support stacking through Cisco StackWise Plus technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

Note The Cisco Catalyst Blade Switch 3032 does not support stacking.

These release notes include important information about Cisco IOS Release 12.2(58)SE and any limitations, restrictions, and caveats that apply to it. 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.

You can download the switch software from this site (registered Cisco.com users with a login password): http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

For the complete list of the Cisco Catalyst Blade Switch 3130 and 3032 for Dell documentation, see the "Related Documentation" section on page 29.

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

Contents

System Requirements

Hardware Supported

Table 1 Cisco Catalyst Blade Switch 3130 for Dell and 3032 for Dell Supported Hardware

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
CBS3032G[1], CBS3130G-S, and CBS3130X-S	• 16 internal Gigabit Ethernet 1000BASE-X downlink ports that connect to the 16 blade servers in the Dell chassis • 4 Gigabit Ethernet (RJ-45) uplink ports • 4 SFP module slots/2 10-Gigabit Ethernet X2 module slots[2] • 1 Ethernet management port (Fa0) used only for switch module management traffic	Cisco IOS Release 12.2(40)EX1

Table 1 Cisco Catalyst Blade Switch 3130 for Dell and 3032 for Dell Supported Hardware (continued)

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco X2 transceiver modules	X2-10GB-SR X2-10GB-LRM X2-10GB-CX4 X2-10GB-LR X2-10GB-LX4	12.2(40)EX3 12.2(46)SE
SFP modules[3]	GLC-T GLC-SX-MM GLC-LH-SM	12.2(40)EX3
Supports OneX (CVR-X2-SFP10G) and these SFP+ modules (For the Catalyst Blade Switch 3130)	SFP-10G-SR Only version 02 or later CX1[4] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	Cisco IOS Release 12.2(55)SE1

1. This switch supports only the IP base software image.
2. X2 supported only on the CBS3130X-S model.
3. SFP = small form-factor pluggable
4. The CX1 cables are used with the OneX converters.

Caution The Cisco Catalyst Blade Switch 3130 for Dell does not support switch stacks with other types of blade switches as members. Combining the Cisco Catalyst Blade Switch 3130 for Dell with other types of blade switches in a switch stack might cause the switch to work improperly or to fail.

Device Manager System Requirements

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, and Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox 1.5, 2.0 or later with JavaScript enabled.

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

Cisco Network Assistant Compatibility

Cisco IOS 12.2(40)EX1 and later is only compatible with Cisco Network Assistant 5.3 and later. You can download Network Assistant from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

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" section on page 4
- "Deciding Which Files to Use" section on page 5
- "Upgrading a Switch by Using the Device Manager or Network Assistant" section on page 6
- "Upgrading a Switch by Using the CLI" section on page 6
- "Recovering from a Software Failure" section on page 7

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 system board flash device (flash:).

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.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base feature set or IP services feature set) and does not change if you upgrade the software license.

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.

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.

Note To use the IPv6 routing and IPv6 ACL features on the Cisco Catalyst Blade Switch 3130 for Dell and 3032 for Dell, you must purchase the IP services software license from Cisco.

Table 3 Cisco IOS Software Image Files

Filename	Description
cbs31x0-universal-tar.122-58.SE1.tar	Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch.
cbs31x0-universalk9-tar.122-58.SE1.tar	Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

The universal software images support multiple feature sets. Use the software activation feature to deploy a software license and to enable a specific feature set. For information about software activation, see the *Cisco Software Activation for Dell* document on Cisco.com:

http://www.cisco.com/en/US/products/ps8742/products_installation_and_configuration_guides_list.html

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 from 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 more 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,* at this URL:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by 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.

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 Download the software image file:

a. If you are a registered customer, go to this URL and log in.

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

b. Navigate to **Switches > Blade Switches.**

c. Navigate to your switch model.

d. Click **IOS Software**, then select the latest IOS release.

Download the image you identified in Step 1.

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 Appendix B in the software configuration guide for this release.

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 switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Software Features

- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate.
- VACL Logging to generate syslog messages for ACL denied IP packets.
- Memory consistency check routine enhancements to detect and correct invalid ternary content addressable memory (TCAM) table entries that can affect switch performance.
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.

- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- NSF IETF mode for OSPFv2—OSPFv2 graceful restart support for IPv4. (IP services feature set only)
- NSF IETF mode for OSPFv3—OSPFv3 graceful restart support for IPv6. (IP services feature set only)
- Support for the Virtual Router Redundancy Protocol (VRRP for IPv4), which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.
- Support for deny ACL entries in Web Cache Communication Protocol (WCCP) redirect lists. Previously only permit entries were supported.

Minimum Cisco IOS Release for Major Features

Table 4 lists the minimum software release (after the first release) required to support the major features of the Catalyst Blade Switch 3130 and 3032 for Dell. Features not listed are supported in all releases.

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Blade Switch Support
Protocol storm protection	12.2(58)SE1	3130 and 3032
VACL logging	12.2(58)SE1	3130 and 3032
Memory consistency check routine enhancements	12.2(58)SE1	3130 and 3032
Smart Call Home	12.2(58)SE1	3130 and 3032
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1	3130 and 3032
Network Time Protocol version 4 (NTPv4)	12.2(58)SE1	3130 and 3032
DHCPv6 bulk-lease query	12.2(58)SE1	3130 and 3032
DHCPv6 relay source configuration	12.2(58)SE1	3130 and 3032
Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.	12.2(58)SE1	3130 and 3032
NSF IETF mode for OSPFv2	12.2(58)SE1	3130 and 3032
NSF IETF mode for OSPFv3	12.2(58)SE1	3130 and 3032
Virtual Router Redundancy Protocol (VRRPv4)	12.2(58)SE1	3130 and 3032
Support for deny ACL entries in Web Cache Communication Protocol (WCCP) redirect lists	12.2(58)SE1	3130 and 3032
Auto-QoS enhancements	12.2(55)SE	3130 and 3032

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Blade Switch Support
Port ACL improvements	12.2(55)SE	3130 and 3032
CDP location enhancements	12.2(55)SE	3130 and 3032
Multi-authentication with VLAN assignment	12.2(55)SE	3130 and 3032
Cisco TrustSec	12.2(55)SE	3130 and 3032
MAC replace to end a session when a host disconnects from a port.	12.2(55)SE	3130 and 3032
Full QoS support for IPv6 traffic.	12.2(52)SE	3130 and 3032
Cisco Medianet to enable intelligent services in the network infrastructure.	12.2(52)SE	3130 and 3032
Support for IP source guard on static hosts.	12.2(52)SE	3130 and 3032
RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated.	12.2(52)SE	3130 and 3032
IEEE 802.1x User Distribution to allow deployments with multiple VLANs.	12.2(52)SE	3130 and 3032
Support for critical VLAN with multiple-host authentication.	12.2(52)SE	3130 and 3032
Customizable web authentication enhancement.	12.2(52)SE	3130 and 3032
Support for Network Edge Access Topology (NEAT).	12.2(52)SE	3130 and 3032
VLAN-ID based MAC authentication.	12.2(52)SE	3130 and 3032
MAC move to allow hosts to move across ports within the same switch.	12.2(52)SE	3130 and 3032
Support for including a hostname in the option 12 field of DHCPDISCOVER packets.	12.2(52)SE	3130 and 3032
DHCP snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE	3130 and 3032
Support for VTP version 3.	12.2(52)SE	3130 and 3032
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE	3130 and 3032
Network Edge Access Topology (NEAT) with 802.1x	12.2(50)SE	3130 and 3032
IEEE 802.1x with open access	12.2(50)SE	3130 and 3032
IEEE 802.1x authentication with downloadable ACLs and redirect URLs	12.2(50)SE	3130 and 3032
Flexible-authentication sequencing of authentication methods	12.2(50)SE	3130 and 3032
Multiple-user authentication on an 802.1x-enabled port.	12.2(50)SE	3130 and 3032
Cisco EnergyWise	12.2(50)SE	3130 and 3032
Wired location service	12.2(50)SE	3130 and 3032
Intermediate System-to-Intermediate System (IS-IS) routing	12.2(50)SE	3130 and 3032
Stack troubleshooting enhancements	12.2(50)SE	3130
CPU utilization threshold trap	12.2(50)SE	3130 and 3032
Embedded Event Manager Version 2.4	12.2(50)SE	3130 and 3032
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling	12.2(50)SE	3130 and 3032
RADIUS server load balancing	12.2(50)SE	3130 and 3032

Table 4 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Blade Switch Support
Auto Smartports Cisco-default and user-defined macros	12.2(50)SE	3130 and 3032
Support for IPv6 features in the IP base and IP services feature sets	12.2(50)SE	3130 and 3032
Voice aware IEEE 802.1x and MAC authentication bypass (MAB) security violation	12.2(46)SE	3130 and 3032
Local web authentication banner	12.2(46)SE	3130 and 3032
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3130
Disabling MAC address learning on a VLAN	12.2(46)SE	3130 and 3032
PAgP Interaction with Virtual Switches and Dual-Active Detection, also referred to as enhanced PAgP	12.2(46)SE	3130 and 3032
Support for rehosting a software license and for using an embedded evaluation software license	12.2(46)SE	3130 and 3032
DHCP server port-based address allocation for the preassignment of an IP address to a switch port	12.2(46)SE	3130 and 3032
HSRP for IPv6	12.2(46)SE	3130
DHCP for IPv6 relay, client, server address assignment and prefix delegation	12.2(46)SE	3130
IPv6 default router preference (DRP)	12.2(46)SE	3130 and 3032
Generic message authentication support with the SSH Protocol and compliance with RFC 4256.	12.2(46)SE	3130 and 3032

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.

- "Cisco IOS Limitations" section on page 10
- "Device Manager Limitations" section on page 17

Cisco IOS Limitations

- "Access Control List" section on page 11
- "Address Resolution Protocol" section on page 11
- "Cisco X2 Transceiver Modules and SFP Modules" section on page 11
- "Configuration" section on page 12
- "EtherChannel" section on page 12
- "HSRP" section on page 13
- "IEEE 802.1x Authentication" section on page 13
- "Multicasting" section on page 14

Access Control List

- The Cisco Catalyst Blade Switch 3130 and 3032 for Dell switches have 964 TCAM entries available for ACLs in the default and routing SDM templates instead of the 1024 entries that are available on the Catalyst 3560 and Catalyst 3750 switches.

  There is no workaround. (CSCse33114)

- When a MAC access list is used to block packets from a specific source MAC address, that MAC address is entered in the switch MAC-address table.

  The workaround is to block traffic from the specific MAC address by using the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command. (CSCse73823)

Address Resolution Protocol

- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.(CSCse06827))

Cisco X2 Transceiver Modules and SFP Modules

- Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number prior to V03 might intermittently fail.

  The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)

- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber).

  Use one of these workarounds:

  - Allow space between the switches when installing them.
  - In a switch stack, plan the SFP module and cable installation so that uplinks in adjacent stack members are not all in use.
  - Use long, small screwdriver to access the latch then remove the SFP module and cable. (CSCsd57938)

- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based IEEE 802.3ae. (CSCsd47344)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

Configuration

- When an excessive number (more than 100 packets per second) of Address Resolution Protocol (ARP) packets are sent to a Network Admission Control (NAC) Layer 2 IP-configured member port, a switch might display a message similar to this:

  ```
  PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism: type 0, class
  51, max_msg 128, total throttled 984323
  -Traceback= 6625EC 5DB4C0 5DAA98 55CA80 A2F2E0 A268D8
  ```

  No workaround is necessary. Under normal conditions, the switch generates this notification when snooping the next ARP packet. (CSCse47548)

- When there is a VLAN with protected ports configured in fallback bridge group, packets might not be forwarded between the protected ports.

  The workaround is to not configure VLANs with protected ports as part of a fallback bridge group. (CSCsg40322)

- When a switch port configuration is set at 10 Mb/s half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the **show controller ethernet-controller** or the **show interfaces** privileged EXEC commands.

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)

- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port.(CSCsi26392)

- If a half-duplex port running at 10 Mb/s receives frames with Inter-Packet Gap (IPG) that do not conform to Ethernet specifications, the switch might stop sending packets.

  There is no workaround. (CSCec74610)

- The bootloader label is incorrect and displays “CISCO DEVELOPMENT TEST VERSION.” However, the actual bootloader software is the correct version with the correct functionality.

  There is no workaround. It does not impact functionality. (CSCta72141)

EtherChannel

- In an EtherChannel running Link Aggregation Control Protocol (LACP), the ports might be put in the suspended or error-disabled state after a stack partitions or a member switch reloads. This occurs when
  - The EtherChannel is a cross-stack EtherChannel with a switch stack at one or both ends.
  - The switch stack partitions because a member reloads. The EtherChannel is divided between the two partitioned stacks, each with a stack master.

The EtherChannel ports are put in the suspended state because each partitioned stack sends LACP packets with different LACP Link Aggregation IDs (the system IDs are different). The ports that receive the packets detect the incompatibility and shut down some of the ports. Use one of these workarounds for ports in this error-disabled state:

- Enable the switch to recover from the error-disabled state.
- Enter the **shutdown** and the **no shutdown** interface configuration commands to enable the port.

The EtherChannel ports are put in the error-disabled state because the switches in the partitioned stacks send STP BPDUs. The switch or stack at the other end of the EtherChannel receiving the multiple BPDUs with different source MAC addresses detects an EtherChannel misconfiguration.

After the partitioned stacks merge, ports in the suspended state should automatically recover. (CSCse33842)

- When a switch stack is configured with a cross-stack EtherChannel, it might transmit duplicate packets across the EtherChannel when a physical port in the EtherChannel has a link-up or link-down event. This can occur for a few milliseconds while the switch stack adjusts the EtherChannel for the new set of active physical ports and can happen when the cross-stack EtherChannel is configured with either mode ON or LACP. This problem might not occur with all link-up or link-down events.

  No workaround is necessary. The problem corrects itself after the link-up or link-down event. (CSCse75508)

- 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)

HSRP

- When the switch stack is in the HSRP active state and a master changeover occurs, you cannot ping the stack by using an HSRP virtual IP address.

  There is no workaround. (CSCth00938)

IEEE 802.1x Authentication

- If a supplicant using a Marvel Yukon network interface card (NIC) is connected an IEEE 802.1x-authorized port in multihost mode, the extra MAC address of 0c00.0000.0000 appears in the MAC address table.

  Use one of these workarounds (CSCsd90495):

  - Configure the port for single-host mode to prevent the extra MAC address from appearing in the MAC address table.
  - Replace the NIC card with a new card.

- When MAC authentication bypass is configured to use Extensible Authentication Protocol (EAP) for authorization and critical authentication is configured to assign a critical port to an access VLAN:

  - If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.

  - If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.

  Use one of these workarounds (CSCse04534):

  - Configure MAC authentication bypass to not use EAP.
  - Define your network access profiles to not use MAC authentication bypass. For more information, see the Cisco Access Control Server (ACS) documentation.

- When IEEE 802.1x authentication with VLAN assignment is enabled, a CPUHOG message might appear if the switch is authenticating supplicants in a switch stack.

  The workaround is not use the VLAN assignment option. (CSCse22791)

Multicasting

- Multicast packets with a time-to-live (TTL) value of 0 or 1 are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the packet belongs to the directly connected network.
  - The TTL value is either 0 or 1.

  The workaround is to not generate multicast packets with a TTL value of 0 or 1, or disable multicast routing in the VLAN. (CSCeh21660)
- Multicast packets denied by the multicast boundary access list are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the multicast packet belongs to a directly connected network.
  - The packet is denied by the IP multicast boundary access-list configured on the VLAN.

  There is no workaround. (CSCei08359)
- Reverse path forwarding (RPF) failed multicast traffic might cause a flood of Protocol Independent Multicast (PIM) messages in the VLAN when a packet source IP address is not reachable.

  The workaround is to not send RPF-failed multicast traffic, or make sure that the source IP address of the RPF-failed packet is reachable. (CSCsd28944)
- If the **clear ip mroute** privileged EXEC command is used when multicast packets are present, it might cause temporary flooding of incoming multicast traffic in the VLAN.

  There is no workaround. (CSCsd45753)
- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value.

  No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)
- When you configure the IGMP snooping throttle limit by using the **ip igmp max-groups** *number* interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number, when all of these conditions are true:
  - The port-channel is configured with member ports across different switches in the stack.
  - When one of the member switches reloads.

  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.

  The workaround is to disable the IGMP snooping throttle limit by using the **no ip igmp max-groups** *number* interface configuration command and then to reconfigure the same limit again. (CSCse39909)

QoS

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.

  There is no workaround. (CSCeh18677)

- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)

- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)

- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)

- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes.

  There is no workaround. (CSCsg79627)

- If QoS is enabled on a switch and the switch has a high volume of incoming packets with a maximum transmission unit (MTU) size greater than 1512 bytes, the switch might reload.

  Use one of these workarounds:

  - Use the default buffer size.
  - Use the **mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* global configuration command to allocate the buffer size. The buffer space for each queue must be at least 10 percent. (CSCsx69718)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

RADIUS

RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

There is no workaround. (CSCta05071)

Routing

- The switch stack might reload if the switch runs with this configuration for several hours, depleting the switch memory and causing the switch to fail:
  - The switch has 400 Open Shortest Path First (OSPF) neighbors.
  - The switch has thousands of OSPF routes.

  The workaround is to reduce the number of OSPF neighbors to 200 or less. (CSCse65252)
- When the PBR is enabled and QoS is enabled with DSCP settings, the CPU utilization might be high if traffic is sent to unknown destinations.

  The workaround is to not send traffic to unknown destinations. (CSCse97660)

SPAN and RSPAN

- When egress SPAN is running on a 10-Gigabit Ethernet port, only about 12 percent of the egress traffic is monitored.

  There is no workaround. This is a hardware limitation. (CSCei10129)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

Stacking

- When using the **logging console** global configuration command, low-level messages appear on both the stack master and the stack member consoles.

  The workaround is to use the **logging monitor** global configuration command to set the severity level to block the low-level messages on the stack member consoles. (CSCsd79037)
- If a new member switch joins a switch stack within 30 seconds of a command to copy the switch configuration to the running configuration of the stack master, the new member might not get the latest running configuration and might not operate properly.

  The workaround is to reboot the new member switch. Use the **remote command all show run** privileged EXEC command to compare the running configurations of the stack members. (CSCsf31301)
- When the flash memory of a stack member is almost full, it might take longer to start up than other member switches. This might cause that switch to miss the stack-master election window. As a result, the switch might fail to become the stack master even though it has the highest priority.

  The workaround is to delete files in the flash memory to create more free space. (CSCsg30073)
- The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:
  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.

  You can use one of these workarounds:
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
  - Remove and reconfigure the VLAN. (CSCsi26444)

- When you use the **switch renumber** global configuration command to renumber a member switch in a switch stack and then reload the switch, the internal server-facing ports do not have the required default of **spanning-tree portfast** enabled.

  The workaround is to apply the switch provision configuration before you reboot the switch. Enter both the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* and the **switch** *stack-member-number* **provision** *type* global configuration commands, and reload the switch. (CSCsl63862)

- If you enter the **show tech-support** privileged EXEC command after you enter the **remote command** {**all** | *stack-member-number*} privileged EXEC command, the complete output does not appear.

  The workaround is to use the **session** *stack-member-number* privileged EXEC command. (CSCsz38090)

VLANs

- When the domain is authorized in the guest VLAN on a member switch port without link loss and an Extensible Authentication Protocol over LAN (EAPOL) is sent to an IEEE 802.1x supplicant to authenticate, the authentication fails. This problem happens intermittently with certain stacking configurations and only occurs on the member switches.

  The workaround is to enter the **shutdown** and **no shutdown** interface configuration commands on the port to reset the authentication status. (CSCsf98557)

- 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)

Device Manager Limitations

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

- If you launch the device manager from a Firefox web browser, an invalid certificate alert appears. If you launch the device manager from an Internet Explorer 7.0 browser, a certificate error appears.

  The workaround when using Firefox is to either temporarily or permanently accept the certificate. If you temporarily accept the certificate, close and then reopen the Firefox browser window. If you permanently accept the certificate, delete the certificate, then close and restart Firefox:

  - If you are using Firefox version 1.5, choose **Tools > Options > Advanced > Security > View Certificates > Web Sites**, select the certificate and click **Delete**.
  - If you are using Firefox version 2.0, choose **Tools > Options > Advanced > Encryption > View Certificates > Web Sites**, select the certificate and click **Delete**.

  The workaround when using Internet Explorer is to click **Click here for Options** in the warning message and click **Display Blocked Content**. Close the browser window and launch a new session. (CSCsk80229)

Important Notes

Cisco IOS Notes

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.

- If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software to Cisco IOS Release 12.2(40)EX1 (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

  ```
  AutoQoS Error: ciscophone input service policy was not properly applied
  policy map AutoQoS-Police-CiscoPhone not configured
  ```

  If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

Device Manager Notes

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.
- 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 enabled 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.

If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.

Open Caveats

- 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.

  Note This does not occur when packets are routed through the switch to another destination.

  There is no workaround.

- CSCtl60247

  When a switch or switch stack 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. If 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, if the switch reloads, the interface loses some 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

- 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.

Resolved Caveats

- CSCsz18045

  When you enter the **show inventory** command on a switch that has an X2 module, the output incorrectly reports the X2 module version ID (VID) as V01 even though the label has a higher VID.

There is no workaround.

- CSCtc72940

  When you reload a stack master, the **ip vrf forwarding** command does not appear in the running configuration, which causes AAA authentication to fail. This issue does not occur with standalone switches.

  The workaround is to reenter the **ip vrf forwarding** command.

- CSCtg00542

  A Link Aggregation Control Protocol (LACP) bundle takes up to 70 seconds to form when NetFlow sampling is enabled.

  The workaround is to disable NetFlow sampling.

- CSCtg11547

  When you configure a switch to send messages to a syslog server in a VPN Routing and Forwarding (VRF) instance, the messages are not sent to the server.

  The workaround is to remove the VRF configuration.

- CSCtg71149

  When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, indicated by the appearance of `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.

  The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

  - Enter the **shutdown** interface configuration command on each member port.
  - Enter the shutdown command on the port-channel interface.
  - Enter the **no shutdown** command on each member port.
  - Enter the **no shutdown** command on the port-channel interface.

- CSCth24267

  A Cisco Catalyst 3130 switch that is a member of a switch stack frequently reports that a redundant power system (RPS) is faulty even though there is no RPS installed and the switch is receiving power from the blade server chassis:

  ```
  Jun  9 13:41:15: %PLATFORM_ENV-1-PWR_RPS: Redundant power supply faulty or in standby
  mode
  Jun  9 13:42:38: %PLATFORM_ENV-1-PWR_RPS: Redundant power supply faulty or in standby
  mode (switchB-2)
  Jun  9 13:46:16: %PLATFORM_ENV-1-PWR_RPS: Redundant power supply faulty or in standby
  mode
  Jun  9 13:47:39: %PLATFORM_ENV-1-PWR_RPS: Redundant power supply faulty or in standby
  mode (switchB-2)
  ```

  Use one of these workarounds to filter the RPS message:

  - Use the **logging discriminator** global configuration command to create a syslog message discriminator.

    For example

    ```
    Switch(config)# logging discriminator filter1 mnemonics drops PWR_RPS
    Switch(config)# logging buffered discriminator filter1
    Switch(config)# logging console discriminator filter1
    ```

```
Switch(config)# logging host ip-address discriminator filter1
```

  - Use the Embedded Syslog Manager (ESM).

- CSCth44403

  When you connect a switch as a VLAN Trunk Protocol (VTP) client to a Catalyst 4000 switch configured as a VTP client or server and the VTP database contains more than 512 VLANs, the database is not correctly updated.

  The workaround is to connect the VTP client directly to a Catalyst 6500 VTP server.

- CSCth71862

  A host switch connected to a stack member switch can download a downloadable access control list (dACL) with more than 13 access control entries, but the dACL is not applied to an interface.

  There is no workaround.

- CSCth88306

  This message appears after inserting the CVR-X2-SFP converter module and the X2-10GB-SR transceiver modules in the10-Gigabit slots of the Catalyst 3750-E and 3560-E switches:

  ```
  %GBIC_SECURITY_CRYPT-4-VN_DATA_CRC_ERROR: GBIC in port Te1/0/1 has bad crc
  ```

  There is no workaround.

- CSCti07994

  When a Catalyst 3750-E or 3560-E switch has a 10/100/1000BASE-TX SFP module installed in a TwinGig SFP Converter Module, and you configure the SFP module to send at 100 Mb/s, save the configuration, and reload the switch, the speed setting is not saved to the running configuration.

  There is no workaround.

- CSCti20222

  On a stack member, the **show interface** command output incorrectly displays a media-type setting.

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

- CSCti27620

  The switch does not generate SNMP traps when a power supply is disconnected.

  There is no workaround.

- CSCti37197

  Enabling the Cisco Discovery Protocol (CDP) on a tunnel interface causes the switch to fail when a a CDP packet is received on the interface.

Note Tunnels are not supported on these platforms.

  The workaround is to use the **no cdp enable** interface configuration command to disable CDP on the interface.

- CSCti45352

  When a FlexLinks backup interface is configured on a member switch in a switch stack, the backup interface incorrectly shows that all VLANs are in the forwarding state.

  The workaround is to use the **show interface trunk** interface configuration command to display the status of the backup link.

- CSCti61145

  When you configure storm control with range command on two interfaces that belong to an EtherChannel group, this message appears:

  ```
  %SYS-3-CPUHOG: Task is running for (2097)msecs, more than (2000)msecs (0/0), process =
  Virtual Exec.
  ```

  The workaround is to configure storm control on a port channel interface.

- CSCti69845

  When MAC Authentication Bypass (MAB) is used in multi-authentication mode, a security violation occurs after successful authentication.

  The workaround is to use a different authentication mode (single, multidomain or multihost).

- CSCti78365

  The config.text.backup file is present after the switch is restored to the factory defaults.

  There is no workaround.

- CSCti95834

  When you enter the **ipv6 traffic-filter** interface configuration command, it might not filter traffic as expected, and it might allow traffic to pass through.

  There is no workaround.

- CSCti95979

  QoS ACL commands might appear differently in the running configuration after the master switch is reloaded or removed from the stack. The functionality of the commands remains the same.

  There is no workaround.

- CSCtj03875

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

  There is no workaround.

- CSCtj25488

  Two stacks that have members with fiber SFP modules are connected in a cross-stack EtherChannel with this configuration:

  - Layer 3 EtherChannels
  - EtherChannel **on** mode

  If a member in one stack is reloaded, this error message appears on a member switch port in the other stack and the port is error disabled.

  ```
  %PLATFORM_PM-3-INTVLANINUSE: internal vlan-id 1012 allocated for interface Gi2/0/2 is
  still in use (3750-b-2)-Traceback= 173E7F0 198F40C 176DA04 1774E70 173FBDC 1744574
  16C9C28 17C65C4 17C67D8 1BB7308 1BADD78 (3750-b-2)
  ```

  The workaround is to configure Layer 2 EtherChannels with SVIs and to use the EtherChannel **Active** mode.

- CSCtj75471

  When a spanning-tree bridge protocol data unit (BPDU) is received on an 802.1Q trunk port and has a VLAN ID is greater than or equal to 4095, the spanning-tree lookup process fails.

  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.

- CSCtj88040

  When a stack is running per-VLAN spanning-tree plus (PVST+) and you create a VLAN, the STP topology change resets the aging time for all members and ages out all the MAC addresses for the new VLAN. If a cookie for the new VLAN on the member is not created when the master sends the member an HRPC message to update the aging timer, the member changes the aging time for VLAN 1 to that set during the topology change.

  After the topology change, the aging time for the new VLAN is reset to that before the STP topology changed. However, the aging time for VLAN 1 does not change. The MAC addresses learned on VLAN 1 and on the member switch ports age out before aging time for the new VLAN.

  The workaround is to disable STP before creating a new VLAN in the stack.

- 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.

- CSCtk11275

  On a switch running Cisco IOS Release 12.2(55)SE with the **parser config cache interface** global configuration command in the configuration, when you use the CISCO-MAC-NOTIFICATION-MIB to enable the SNMP MAC address notification trap, the trap is enabled, but the trap setting does not appear in the switch configuration.

  The workaround is to remove the **parser config cache interface** command from the configuration.

- CSCtk13113

  The CPU usage on a standalone switch varies as the switch updates the running configuration.

  There is no workaround.

- CSCtk32638

  When the switch stack elects a new stack master, by default the MAC address of the new master becomes the stack MAC address. Configuring a persistent MAC address sets a delay after stack master change before the stack master MAC address change. A timer value of 0 means that the MAC address of the current master is used indefinitely.

  When you enter the **stack-mac persistent timer 0** global configuration command on a stack and the master switch is not the original owner of the stack MAC address, ports on member switches do not go through Rapid Spanning Tree Protocol (STP) transitions directly into the forwarding state.

  The workaround is to not use the **stack-mac persistent timer 0** command on the switch stack.

- CSCtl42740

  When 802.1x MAC authentication bypass with multidomain authentication and critical VLAN are enabled on an interface on a switch running Cisco IOS Release 12.2(53)SE or later, if the switch loses connectivity with the AAA server, the switch might experience high CPU usage and show these messages:

  ```
  AUTH-EVENT (Gi0/15) Received clear security violation
  ```

```
AUTH-EVENT (Gi0/15) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on port
GigabitEthernet0/15
```

There is no workaround.

- 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.

- CSCtl80678

  The port manager callback might cause more than 90% CPU usage for up to 20 minutes under these conditions:

  - Link comes up simultaneously on multiple dot1q trunk ports.
  - VLAN Trunking Protocol (VTP) pruning is enabled.

  The workaround is to disable VTP pruning.

- CSCtn57224

  The switch sends temperature trap messages when its temperature is between 58 and 60° C.

  There is no workaround.

- CSCto62631

  A switch running Cisco IOS Release 12.2(58)SE might reload if:

  - 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 prior to Cisco IOS Release 12.2(58)SE.

Documentation Updates

Note The “Supported MIBs” appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Updates to the Switch Getting Started Guide

When you launch Express Setup, you are prompted for the switch password. Enter the default password, *cisco*. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, *cisco*.

Updates to the Software Configuration Guide

Correction to the "Configuring STP" Chapter

In the "Displaying the Spanning-Tree Status" section of the "Configuring STP" chapter, this note should appear:

Note In a switch stack, the spanning-tree process reports both physical stack ports in a stack member as one logical port.

Correction to the "Configuring Network Security with ACLs" Chapter

The "Creating a Numbered Extended ACL" section of the "Configuring Network Security with ACLs" chapter has an error. Contrary to the note in this section, ICMP echo-replies can be filtered.

Correction to the "Unsupported Commands" Chapter

The "Miscellaneous" section of the "Unsupported Commands" chapter should include the **logging discriminator** global configuration command.

Updates for the System Message Guide

New System Messages

Error Message `IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]`

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-ARP: vlan [dec] (port [chars]) denied arp ip [inet] -> [inet], [dec] packet[chars]`

Explanation A packet from the virtual LAN (VLAN) that matches the VLAN access-map (VLMAP) log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-L4: vlan [dec] (port [chars]) denied [chars] [inet]([dec]) -> [inet]([dec]), [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the second [chars] is the protocol, the first [inet] is the source IP address, the second [dec] is the source port, the second [inet] is the destination IP address, the third [dec] is the destination port, the fourth [dec] denotes the number of packets, and the third [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-IGMP: vlan [dec] (port [chars]) denied igmp [inet] -> [inet] ([dec]), [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] is the Internet Group Management Protocol (IGMP) message type, the third [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-ICMP: vlan [dec] (port [chars]) denied icmp [inet] -> [inet] ([dec]/[dec]), [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the first [inet] is the source IP address, the second [inet] is the destination IP address, the second [dec] is the Internet Control Message Protocol (ICMP) message type, the third [dec] is the ICMP message code, the fourth [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `VLMAPLOG-6-IP: vlan [dec] (port [chars]) denied ip protocol=[dec] [inet] -> [inet], [dec] packet[chars]`

Explanation A packet from the VLAN that matches the VLMAP log criteria was detected. The first [dec] is the VLAN number, the first [chars] is the port name, the second [dec] is the protocol number, the first [inet] is the source IP address, the second [inet] is the destination IP address, the third [dec] denotes the number of packets, and the second [chars] represents the letter "s" to indicate more than one packet.

Recommended Action No action is required.

Error Message `AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]`

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars]s is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Modified System Messages

Error Message `AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]`

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message `AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])`

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Error Message `MAB-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was unsuccessful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `MAB-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was successful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Deleted System Messages

Error Message `IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST`

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

Related Documentation

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

These documents provide complete information about the Cisco Catalyst Blade Switch 3130 and 3032 for Dell and are available from this Cisco.com site:
http://www.cisco.com/en/US/products/ps6748/tsd_products_support_series_home.html

- *Cisco Catalyst Blade Switch 3130 for Dell and Cisco Catalyst Blade Switch 3032 for Dell Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3000 Series for Dell*
- *Release Notes for the Cisco Catalyst Blade Switch 3130 and 3032 for Dell*

Note Before you install, configure, or upgrade the switch module, see the release notes on Cisco.com for the latest information.

- *Cisco Catalyst Blade Switch 3130 and 3032 for Dell Software Configuration Guide*
- *Cisco Catalyst Blade Switch 3130 and 3032 for Dell Command Reference Cisco Catalyst Blade Switch 3130 and 3032 for Dell System Message Guide* (not orderable but available on Cisco.com)

- *Cisco Software Activation Document for Dell*
- These compatibility matrix documents are available from this Cisco.com site: http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation and Submitting a Service Request

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.