Release Notes for Cisco Catalyst Blade Switch 3120 for HP, Cisco IOS Release 15.0(2)SE and Later

December 04, 2015

Cisco IOS Release 15.0(2)SE and later runs on the Cisco Catalyst Blade Switch 3120 for HP switches. These switches support stacking through Cisco StackWise Plus technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about Cisco IOS Release 15.0(2)SE and later 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 4.

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 3120 for HP documentation, see the "Related Documentation" section on page 30.

Note References in this document to the CBS3120G-S and CBS3120X-S switches also apply to the CBS3125G-S and CBS3125X-S switches, respectively.

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 3120 for HP Supported Hardware

Switch Hardware	Description	Minimum Cisco IOS Release
CBS3120G-S and CBS3120X-S	• 18 internal Gigabit Ethernet 1000BASE-X downlink ports that connect to the blade enclosure. • 4 Gigabit Ethernet (RJ-45) uplink ports • 4 RJ-45 SFP module slots[1]/ 2 10-Gigabit Ethernet X2 module slots • 1 Ethernet management port (Fa0) used only for switch module management traffic	12.2(40)EX1
Cisco X2 transceiver modules	X2-10GB-SR X2-10GB-LRM X2-10GB-CX4	12.2(40)EX3
	X2-10GB-LR X2-10GB-LX4	12.2(46)SE
SFP modules[2]	GLC-T GLC-SX-MM GLC-LH-SM	12.2(40)EX3

Table 1 Cisco Catalyst Blade Switch 3120 for HP Supported Hardware (continued)

Switch Hardware	Description	Minimum Cisco IOS Release
Supports OneX (CVR-X2-SFP10G) and these SFP+ modules	SFP-10G-SR Only version 02 or later CX1[3] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(55)SE1

[1] X2 module supported only on the CBS3120X-S model

[2] SFP = small form-factor pluggable

[3] The CX1 cables are used with the OneX converters.

Caution The Cisco Catalyst Blade Switch 3120 for HP switch modules do not support switch stacks with other types of blades switches as members. Combining the Cisco Catalyst Blade Switch 3120 for HP 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, page 3
- Software Requirements, page 3

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 Release 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, page 4
- Deciding Which Files to Use, page 4
- Upgrading a Switch by Using the Device Manager or Network Assistant, page 6
- Upgrading a Switch by Using the CLI, page 6
- Recovering from a Software Failure, 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.

Note To use the IPv6 routing and IPv6 ACL features on the Cisco Catalyst Blade Switch 3120 for HP, you must purchase the IP services software license from Cisco.

Table 3 Cisco IOS Software Image Files

Filename	Description
cbs31x0-universal-tar.150-2.SE.tar	Cisco Catalyst Blade Switch 3120 for HP 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.150-2.SE1.tar	Cisco Catalyst Blade Switch 3120 for HP 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 HP* document on Cisco.com:

http://www.cisco.com/en/US/products/ps6748/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/cbs31x0-universal-tar.122-40.EX1.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

New in Cisco IOS Release 15.0(2)SE1

- Support for Right-To-Use (RTU) licensing, which allows you to upgrade from one license level to another by entering commands in the command line interface without interacting with the Cisco Product License Registration portal.

New in Cisco IOS Release 15.0(2)SE

- Support for OSPFv3 authentication with IPsec. You can now use the IPsec secure socket API to authenticate OSPF for IPv6 (OSPFv3) packets to ensure that the packets are not altered and resent to the switch. For more information, see the *IPv6 Unicast Routing* chapter of the software configuration guide on Cisco.com. (Switches running the IP Base image)
- Support for IPv6 multicast. For more information, see the *Implementing IPv6 Multicast* chapter of the software configuration guide on Cisco.com.

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 3120 for HP. 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
IPv6 multicast support	15.0(2)SE
Protocol storm protection	12.2(58)SE1
VACL logging	12.2(58)SE1
Memory consistency check routine enhancements	12.2(58)SE1
Smart Call Home	12.2(58)SE1
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1
Network Time Protocol version 4 (NTPv4)	12.2(58)SE1
DHCPv6 bulk-lease query	12.2(58)SE1
DHCPv6 relay source configuration	12.2(58)SE1
Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.	12.2(58)SE1
NSF IETF mode for OSPFv2	12.2(58)SE1
NSF IETF mode for OSPFv3	12.2(58)SE1
Virtual Router Redundancy Protocol (VRRPv4)	12.2(58)SE1
Support for deny ACL entries in Web Cache Communication Protocol (WCCP) redirect lists	12.2(58)SE1
Auto-QoS enhancements	12.2(55)SE
Port ACL improvements	12.2(55)SE
CDP location enhancements	12.2(55)SE
Multi-authentication with VLAN assignment	12.2(55)SE
Cisco TrustSec	12.2(55)SE
MAC replace to end a session when a host disconnects from a port.	12.2(55)SE
Full QoS support for IPv6 traffic.	12.2(52)SE
Cisco Medianet to enable intelligent services in the network infrastructure for video applications.	12.2(52)SE
Support for IP source guard on static hosts.	12.2(52)SE
RADIUS Change of Authorization (CoA)	12.2(52)SE
IEEE 802.1x User Distribution	12.2(52)SE
Critical VLAN with multiple-host authentication	12.2(52)SE
Customizable web authentication enhancement	12.2(52)SE
NEAT to change the port host mode and to apply a standard port configuration on the authenticator switch port	12.2(52)SE
VLAN-ID based MAC authentication	12.2(52)SE
MAC move	12.2(52)SE
Support for including a hostname in the option 12 field of DHCPDISCOVER packets	12.2(52)SE

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

Feature	Minimum Cisco IOS Release Required
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
Support for VTP version 3.	12.2(52)SE
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE
Network Edge Access Topology (NEAT) with 802.1x	12.2(50)SE
IEEE 802.1x with open access	12.2(50)SE
IEEE 802.1x authentication with downloadable ACLs and redirect URLs	12.2(50)SE
Flexible-authentication sequencing of authentication methods	12.2(50)SE
Multiple-user authentication on an 802.1x-enabled port.	12.2(50)SE
Cisco EnergyWise	12.2(50)SE
Wired location service	12.2(50)SE
Intermediate System-to-Intermediate System (IS-IS) routing	12.2(50)SE
Stack troubleshooting enhancements	12.2(50)SE
CPU utilization threshold trap	12.2(50)SE
Embedded Event Manager Version 2.4	12.2(50)SE
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling	12.2(50)SE
RADIUS server load balancing	12.2(50)SE
Auto Smartports Cisco-default and user-defined macros	12.2(50)SE
Support for IPv6 features in the IP base and IP services feature sets	12.2(50)SE
Voice aware IEEE 802.1x and MAC authentication bypass (MAB) security violation	12.2(46)SE
Local web authentication banner	12.2(46)SE
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE
Disabling MAC address learning on a VLAN	12.2(46)SE
PAgP Interaction with Virtual Switches and Dual-Active Detection, also referred to as enhanced PAgP	12.2(46)SE
Support for rehosting a software license and for using an embedded evaluation software license	12.2(46)SE
DHCP server port-based address allocation for the preassignment of an IP address to a switch port	12.2(46)SE
HSRP for IPv6	12.2(46)SE
DHCP for IPv6 relay, client, server address assignment and prefix delegation	12.2(46)SE
IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router.	12.2(46)SE
Generic message authentication support with the SSH Protocol and compliance with RFC 4256.	12.2(46)SE

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

Access Control List

- The Cisco Catalyst 3120 for HP Blade Switch has 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

- Cisco X2-10GB-LR transceiver modules with a version identification number lower than V03 might show intermittent frame check sequence (FCS) errors or be ejected from the switch during periods of operational shock greater than 50 g.

  There is no workaround. (CSCse14048)
- Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number before 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 a long, small screwdriver to access the latch, and 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 on IEEE 802.3ae. (CSCsd47344)

Configuration

- 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)
- 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)
- 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)
- An internal switch port is down when one of these HP Flex 10-Gigabit Ethernet network interface cards (NICs) is up:
  - Flex 522m Mezz
  - Flex 542m Mezz
  - Flex 552m Mezz

  The workaround is to use the **speed nonegotiate** interface configuration command on the internal port. (CSCth94904)

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 to 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 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.
  - 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)

Quality of Service (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 **shut** and **no shut** 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 start.

  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, and 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, page 18
- Device Manager Notes, page 18

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 interfaces 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.
- We recommend this browser setting to reduce 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.

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

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.

- 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.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.0(2)SE9

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*

Bug ID	Headline
CSCtn75051	%SYS-3-TIMERNEG: Cannot start timer with negative offset
CSCul01067	Memory leak in NTP client with IPv6 configuration
CSCus13476	CSR handled only one MACSec interface's authentication
CSCus40723	No simulated EAP success message to the client for credential failure
CSCut20271	C3560X responds to ARP request from management port
CSCuu28768	C2960 ARP Table adding MACs on Incorrect Interface
CSCuu41771	Members in a 2960 cluster unable to save configuration in IOS 15.x
CSCuv05123	c3560e/v151_sy_throttle platform doesn't store NTP drift values properly
CSCuv94875	SmartPort Macro with SCP not working

Caveats Resolved in Cisco IOS Release 15.0(2)SE8

Use the Bug Search Toolkit to view the details of a caveat listed in this section. For more information about the BST, go to *https://tools.cisco.com/bugsearch/*

Bug ID	Headline
CSCtq21722	SNMP crash forced due to an invalid memory block
CSCuo66933	Switch sent Failure packet after reboot and caused PC to fail authenticate
CSCue80816	Crash while routine config push through SNMP
CSCud65150	Crash after Kron runs a TCL script
CSCtx23014	HSRP hellos cannot be sourced from certain IPs for specific vlan
CSCuo31164	match prefix is removed from SNMP V3 configuration after host command
CSCum75962	abnormal dot1x authentication failure msg from some specific mac address
CSCuq85748	dot1x authorization fails, when we recovering from Guest VLAN
CSCum65703	Inconsistency on config "privilege" commands as seen in running-config
CSCsq42459	No log message of falling the cpu threshold
CSCuh46221	EEM Tcl policies fail due to false out of memory error
CSCtj17637	MF: HTTPS generates a new self-signed cert on reboot even if one exists

Bug ID	Headline
CSCud66899	IOS supplicant: ACS5 authc fail for PEAPv1/MSCHAPv2
CSCur58372	"snmp-server enable traps syslog" still in "show run all" after removal
CSCui43116	dot1x State Radius AV pair not send while failing over between AAA grps
CSCur76305	Memory leak in ASP proces Catalyst 2960s
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCur50403	LOGIN_FAILED log message should not display the bad username
CSCur74187	Device sending Client IP address as "Calling-Station-Id" with WebAuth
CSCut05808	UDP(1975) causes Error msg %IPC-2-INVALIDZONE

Caveats Resolved in Cisco IOS Release 15.0(2)SE7

- CSCun80959

  Designated port on the Root Bridge experiences a block forward for 30 seconds. This issue occurs because the message-time (the period of time a packet is alive in the network) is almost equal to max-age (the period of time a packet is allowed to stay in the network). When message-time >= max-age, the switch receives an agedMsg on the forwarding port which moves the port to a blocking state.

  There is no workaround.

- CSCup32608

  Link State Tracking (LST) fails after upgrade to Cisco IOS Release 15.0(2)SE6. The LST downstream interfaces flap continually while the upstream interfaces remain stable.

  The workaround is to disable Link State Tracking on the switch. Alternatively, downgrade to Cisco IOS Release 15.0(2) SE5.

- CSCup61889

  Due to a timing issue, the port channel member port on the slave switch of the stack loops during boot up. The issue occurs only on the member port that is configured as the first port in a cross-stack EtherChannel configuration and when Nexus devices are connected to Cisco devices. Due to Link Aggregation Control Protocol (LACP) graceful convergence, when both the devices are up and in sync (S) state, Cisco devices start transmitting even before the devices get onto collecting (C) state. This causes the port to be pulled down by the Nexus devices. When this happens during boot up, the EtherChannel hardware programming for the port is cleared even when the port is bundled in the port-channel.

  The workaround is to enter the **shutdown/no shutdown** command on the port-channel interface or disable lacp graceful-convergence on the port-channel on peer devices.

- CSCup86666

  An interface configured with **no logging event link-status** command, fails to change its state from disabled to enabled when you run the **logging event link-status** command along with the **switchport** command.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE6

- CSCue95644

  When you upgrade a device to a Cisco IOS or Cisco IOS XE release that supports Type 4 passwords, enable secret passwords are stored using a Type 4 hash which can be more easily compromised than

  The workaround is to configure the **enable secret** command on an IOS device without Type 4 support, copy the resulting Type 5 password, and paste it into the appropriate command on the upgraded IOS

  device.

- CSCuf05034

  The workaround is to use chassisTempAlarm object from CISCO-STACK-MIB to get the following values:

  - off — when the temperature of the device is in normal range
  - on — when the temperature of the device is too high
  - critical — when the temperature of the device is critical due to which a system shut down is imminent.

- CSCuh51379

  When VTp mode is set to transparent and vlan.dat file present in flash is deleted, after reload, access vlan is not configured in the switch even though vlan configuration is present in running config or startup config.

  The workaround is to set the vtp mode to server or client.

- CSCuj81498

  The internal port links between 3020 switches and blade servers do not work when you start the switch and the server with a specific power on and off sequence.

  The workaround is to restart the switch.

- CSCto13462

  In a network that consists of two DHCP clients with same client id and different mac addresses, the DHCP server reloads when one of the clients releases its DHCP address.

  There is no workaround.

- CSCts80209

  A switch configured with login quiet-mode resets when you enter the **login block-for** or **no login block-for** commands.

  There is no workaround. To avoid a reset, do not enter the **login block** or **no login block-for** command.

Caveats Resolved in Cisco IOS Release 15.0(2)SE5

- CSCua00661

  A memory leak is observed when configuring VLANs using tclsh mode.

  The workaround is to make the tclsh mode interactive to avoid any memory leak.

- CSCue94252

When the **privilege exec level 5 show mac address-table interface gigabitethernet** privileged EXEC command is entered, all interfaces in the switch have the command applied to the running configuration.

There is no workaround.

- CSCug26848

  CPU usage goes above 90% when Internet Group Management Protocol (IGMP) version 3 report packets are sent to the switch which has IGMP version 2 configured on the switch virtual interface.

  The workaround is to either disable multicast fast convergence or configure IGMP version 3 on switch virtual interface.

- CSCug51225

  Topology Change Notification (TCN) occurs over the network when a new stack member is added to the switch stack.

  There is no workaround

- CSCug52714

  TACACS+ single connect authentication request from a switch stack takes around 10 to 12 minutes to failover to secondary server after the primary TACACS server is unreachable.

  The workaround is to disable TACACS+ single connect configuration on the switch.

- CSCuh75095

  After rebooting a Cisco Catalyst Blade Switch 3012 (CBS3012), incorrect data is found in the vital product data (VPD) of the switch, which causes the switch to become unmanageable.

  There is no workaround.

- CSCui41032

  Switch runs out of memory within few seconds of configuring the command **privilege exec level <n> show spanning-tree active/detail**.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE4

- CSCuf77683

  Internal VLANs are displayed when the **show snmp mib ifmib ifindex** command is entered or the SNMP is queried for the ipMIB object.

  The workaround is to check if the displayed VLANs are internal and then to hide them.

- CSCug62154

  When the switch is started using TACACS+ configurations, the CPU utilization increases to 100% and the VTY device does not work.

  The workaround is to remove the TACACS+ configurations and restart the switch.

- CSCuh41077

  The ipAddrEntry value in the IP Address Table shows an interface index that is not exposed by the ifEntry Object ID.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE3

- CSCta43825

  CPU usage is high when an SNMP Walk of the Address Resolution Protocol (ARP) table is performed.

  The workaround is to implement SNMP view using the following commands:

  snmp-server view cutdown iso included

  snmp-server view cutdown at excluded

  snmp-server view cutdown ip.22 excluded

  snmp-server community public view cutdown ro

  snmp-server community private view cutdown rw

- CSCts95370

  If an ACL is configured on a router VTY line for ingress traffic, the ACL is applied for egress traffic also. As a result, egress traffic to another router on an SSH connection is blocked.

  The workaround is to permit egress traffic to the specific destination router using the **permit tcp host** <*destination router IP address*> **eq 0 any** interface configuration command.

- CSCub85948

  Memory leak is seen in the switch when it sends CDP, LLDP or DHCP traffic and when the link flaps.

  The workaround is to apply protocol filters to the device sensor output by entering the following global configuration commands:

  no macro auto monitor

  device-sensor filter-spec dhcp exclude all

  device-sensor filter-spec lldp exclude all

  device-sensor filter-spec cdp exclude all

  If the memory leak continues in the "DHCPD Receive" process, disable the built-in DHCP server by entering the **no service dhcp** global configuration command.

- CSCuc40634

  STP loop occurs on Flexstack connected by parallel links when a link state is changed on Flexlink port.

  The workaround is to change the switch to root bridge.

- CSCud96215

  LSG Downlink port flaps when SFP+ is used as an uplink port. This issue also appears if SFP+ is configured in a flexlink configuration.

  There is no workaround. The configuration recovers automatically.

- CSCud83248

  When native VLAN is configured on the trunk or when switchport trunk native vlan 99 is configured on the interface, spanning-tree instance is not created for native VLAN.

The workaround is to keep VLAN1 as a native on the trunk. In Cisco IOS Release15.0(2) SE, **dot1.x** is enabled by default and causes authentication fail in the native VLAN. This results in **pm_vp_statemachine** not triggering any event to spanning tree. To disable **dot1x** internally, run the **no macro auto monitor** command. The stp instance is created for native vlan 99 after running the **show** and **no show** command on the interface.

- CSCue87815

  When the secret password is configured, the password is not saved. The default password is used as the secret password.

  The workaround is to use the default password to login and then change the password.

Caveats Resolved in Cisco IOS Release 15.0(2)SE1

- CSCee32792

  When using SNMP v3, the switch unexpectedly reloads when it encounters the snmp_free_variable_element.

  There is no workaround.

- CSCth03648

  When two traps are generated by two separate processes, the switch fails if one process is suspended while the other process updates variables used by the first process.

  The workaround is to disable all SNMP traps.

- CSCth59458

  If a redundant power supply (RSP) switchover occurs during a bulk configuration synchronization, some of the line configurations might disappear.

  The workaround is to reapply the line configurations.

- CSCtl12389

  The **show ip dhcp pool** command displays a large number of leased addresses.

  The workaround is to turn off **ip dhcp remember** and reload the switch.

- CSCtq64716

  The following warning messages might be displayed during the boot process even when a RADIUS or a TACACS server have been defined:

  ```
  %RADIUS-4-NOSERVNAME:
  ```

  or

  ```
  %AAAA-4-NOSERVER: Warning: Server TACACS2 is not defined
  ```

  There is no workaround.

- CSCtr37757

  The secure copy feature (**copy:** *source-filename* **scp**: *destination-filename* command) does not work.

  There is no workaround.

- CSCtt41416

  The **show switch chassis management** command incorrectly displays all slot numbers as 0.

  There is no workaround.

- CSCtz98066

  When the master switch (Switch A) is reloaded or loses power and rejoins the stack as a member switch, any traffic stream that exits Switch A is dropped because the newly joined member is not able to establish an Address Resolution Protocol (ARP) entry for the next hop router or switch. Debugs confirm that Switch A does not send a GARP or ARP for the next hop, though traffic continues to be sent to the switch.

  The workaround is to add a static ARP. Ping the destination from Switch A to force the ARP to respond.

- CSCtz99447

  Local web authorization and HTTP services on the switch do not respond because of a web authorization resource limitation in the system. The resource limitation is normally caused by incorrectly terminated HTTP or TCP sessions.

  These are possible workarounds and are not guaranteed to solve the problem:

  - Enter the **ip admission max-login-attempts** privileged EXEC command to increase the number of maximum login attempts allowed per user.
  - If the web authorization module is intercepting HTTP sessions from web clients in an attempt to authorize them, try using a different browser.
  - Eliminate background processes that use HTTP transport.

- CSCua54224

  Heavy traffic load conditions may cause the loop guard protection function to be automatically activated and almost immediately deactivated. These conditions can be caused by entering the **shutdown** and **no shutdown** interface configuration commands or by interface link flaps on more than forty ports. These log messages appear:

  ```
  %SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet1/0/1 on MST0.
  %SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet1/0/1 on
  MST0.
  ```

  There is no workaround.

- CSCua87594

  When a peer switch sends inferior Bridge Protocol Data Units (BPDUs) on the blocking port of the Cisco switch (with the proposal bit ON), the Cisco switch waits for three such BPDUs before responding with a better BPDU. This leads to a convergence time of more than 5 seconds. The problem appears under these conditions:

  - The Cisco switch is not configured as the root switch.
  - The Cisco switch uses Multiple Spanning-Tree Protocol (MSTP) and the peer switch uses Rapid Spanning Tree Protocol (RSTP) or rapid per-VLAN spanning-tree plus (rapid PVST+).

  There is no workaround.

- CSCub14238

  With switches running Cisco IOS Release 15.0(2)SE, there was a problem when port-based address allocation was configured. The DHCP client did not receive IP addresses from the server if the client ID was configured as an ASCII string or if the subscriber ID was used as the client ID.

  This problem has been fixed now. No action is required.

- CSCub14641

  When you configure and save the monitor session source interface, the configuration is not saved after reboot.

There is no workaround.

- CSCub93357

  If an interface is configured with the **switchport port-security maximum 1 vlan** command, the following error message is displayed:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
  address XXXX.XXXX.XXXX on port <interface>
  ```

  There is no workaround.

- CSCuc03555

  The flash memory is corrupted when you format the flash manually.

  The workaround is to reload the switch. (Note that this will erase the flash memory, and you will need to reload the software image using TFTP, a USB drive, or a serial cable.

- CSCuc17720

  If the Performance Monitor cache is displayed (using the **show performance monitor cache** command) and you attempt to stop the command output display by entering the **q** keyword, there is an unusually long delay before the output is stopped.

  The workaround is to enter the **term len 0** privileged EXEC command so that all command outputs are displayed without any breaks.

Caveats Resolved in Cisco IOS Release 15.0(2)SE

- CSCto78529

  After upgrading to Cisco IOS Release 12.2(58)SE1, the Fa0 port on the switch does not respond to the **ping** command.

  The workaround is to use Cisco IOS Release 12.2(55)SE.

- CSCtq38500

  When an interface is configured with the **mls qos** command, traffic is not matched by port-based QoS ACLs that use the range option.

  The workaround is to is to configure the switch using the single port eq keyword. Alternatively, you can configure the trust under class-default setting for the same policy-map that uses the acl-range option.

- CSCtq51049

  In a switch stack, you cannot establish a console session with a member switch when an ACL is applied to the VTY lines.

  The workaround is to use the following procedure when you apply an ACL to line vty 0 4 and line vty 5 15:

  1. Create the **vty** ACL and permit the 127 network.
  2. Append the **vrf-also** keyword to the configured access-class inbound.

  See the following example:

  ```
  ip access-list standard vty-acl
     permit 127.0.0.0 0.0.0.255

  line vty 0 4
     access-class vty-acl in vrf-also
     privilege level 15
  ```

```
   length 0
   transport input ssh
line vty 5 15
   access-class vty-acl in vrf-also
   privilege level 15
   transport input ssh
```

- CSCtr07908

  The archive download feature does not work if the flash contains an “update” directory. This situation is likely to occur if a previous download failed or was interrupted and the “update”” directory is still left in the flash.

  The workaround is to delete the “update” directory in the flash before starting the archive download.

- CSCtr44361

  When a device is moved from one port to another in a switch stack, the SNMP data generated for the move event is incorrect.

  The workaround is to ensure that the uplink to the core network is configured on the master switch (for example, a 1/0/x port).

- CSCtr55645

  OSPFv3 neighbors might flap because of the way the switch handles IPv6 traffic destined for well-known IPv6 multicast addresses.

  There is no workaround.

- CSCts36715

  Users connecting to the network through a device configured for web proxy authentication may experience a web authentication failure.

  There is no workaround. Use the **clear tcp tcb** command to release the HTTP Proxy Server process.

- CSCtt11621

  Using the **dot1x default** command on a port disables access control on the port and resets the values of the **authentication host-mode** and **authentication timer reauthenticate** commands to the default values.

  The workaround is to avoid using the **dot1x default** command and set various dot1x parameters individually. You can also reconfigure the parameters that were changed after you entered the **dot1x default** command.

- CSCtx33436

  When using the **switchport port-security maximum** 1 **vlan access** command, if an IP-phone with a personal computer connected to it is connected to an access port with port security, a security violation will occur on the interface. This type of message is displayed on the console:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
  XXXX.XXXX.XXXX on port FastEthernet0/1.
  ```

  Here is a sample configuration:

  ```
  interface gigabitethernet 3/0/47
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 3
  switchport port-security maximum 2
  switchport port-security maximum 1 vlan access
  switchport port-security maximum 1 vlan voice
  switchport port-security
  ```

The workaround is to remove the line **switchport port-security maximum** 1 **vlan access**.

- CSCtx96491

  The switch does not correctly detect a loopback when the switch port on an authenticated IP phone is looped to a port configured and authenticated with dot1x security, even when **bpduguard** is configured on the interface. This situation can result in 100 percent CPU utilization and degraded switch performance.

  The workaround is to configure the interface with the **authentication open** command or to configure **authentication mac-move permit** on the switch.

- CSCue23882

  If a new port is added to an etherchannel on a switch using DAI or IPDT, ARP packets that ingress the port are lost.

  The workaround is to save the configuration and reload the switch. Alternatively, configure the switch by entering the **no macro auto monitor** command followed by the **macro auto monitor** command after the port is bundled for the first time.

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 3120 for HP Blade Switch 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 3000 Series for HP Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3000 Series for HP*
- *Release Notes for the Cisco Catalyst Blade Switch 3120 for HP*

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 3120 for HP Software Configuration Guide*
- *Cisco Catalyst Blade Switch 3120 for HP Command Reference*
- *Cisco Catalyst Blade Switch 3120 for HP System Message Guide*
- *Cisco Software Activation Document for HP*
- 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*

For other information about related products, see these documents on Cisco.com:

- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Network Admission Control Software Configuration Guide*

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, at:

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.