Release Notes for the Cisco Catalyst Blade Switch 3020 for HP, Cisco IOS Release 15.0(2)SE and Later

August 31, 2018

These release notes include important information about Cisco IOS Release 15.0(2)SE and any limitations, restrictions, and caveats that apply to them. 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 switch packaging.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 3.
- 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 3.

For the complete list of Cisco Catalyst Blade Switch 3020 for HP documentation, see the "Related Documentation" section on page 24.

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

Contents

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

- "Resolved Caveats" section on page 13
- "Related Documentation" section on page 24
- "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page 24

System Requirements

- "Hardware Supported" section on page 2
- "Device Manager System Requirements" section on page 2

Hardware Supported

Table 1 Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
Cisco Catalyst Blade Switch 3020 for HP	24-Gigabit Ethernet ports and 4 SFP module slots	Cisco IOS Release 12.2(35)SE
Small form factor pluggable (SFP) modules	1000BASE-LX and -SX	Cisco IOS Release 12.2(35)SE

Device Manager System Requirements

- "Hardware Requirements" section on page 2
- "Software Requirements" section on page 2

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.

Upgrading the Switch Software

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.

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 If you wish to use Device Manager to upgrade the switch from Cisco IOS Release 12.2(35)SE through Cisco IOS Release 12.2(40)SE1 (the LAN Base image) to Cisco IOS Release 12.2(50)SE or later (the IP base image), you must first upgrade to Cisco IOS Release 12.2(40)SE2.

Table 3 lists the filenames for this software release.

Table 3 Cisco IOS Software Image Files

Filename	Description
cbs30x0-ipbase-tar.150-2.SE.tar	Cisco Catalyst Blade Switch 3020 for HP image file and device manager files. This image has Layer 2+ features.
cbs30x0-ipbasek9-tar.150-2.SE.tar	Cisco Catalyst Blade Switch 3020 for HP cryptographic image file and device manager files. This image has the Kerberos and SSH features.

Archiving Software Images

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

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for 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

You can upgrade switch software by using the device manager. 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 3 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 or the HP Onboard Administrator program described in the getting started guide.
- The CLI-based setup program, as described in the hardware installation guide.
- The DHCP-based autoconfiguration, as described in the software configuration guide.
- Manually assigning an IP address, as described in the software configuration guide.

New Software Features

- 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..
- Support for port security on Etherchannels. For more information, see the *Configuring Port-Based Traffic Control* chapter in the software configuration guide.

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 6
- "Device Manager Limitations" section on page 11

Cisco IOS Limitations

- "Bootloader" section on page 6
- "Ethernet" section on page 7
- "IP" section on page 8
- "IP Telephony" section on page 8
- "Multicasting" section on page 8
- "Quality of Service (QoS)" section on page 9
- "SPAN and RSPAN" section on page 9
- "Trunking" section on page 10
- "VLAN" section on page 10

Bootloader

- 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)

Configuration

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

  This problem occurs under these conditions:

  - When the switch is booted without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).

  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mp/s full duplex or 100 Mp/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mp/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

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

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

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

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

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

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

- 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)

Ethernet

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream might map to same member ports, based on hashing results calculated by the ASIC.

  If this happens, traffic distribution is uneven on EtherChannel ports.

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:
  - for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
  - for incrementing source-ip traffic, configure load balance method as **src-ip**
  - for incrementing dest-ip traffic, configure load balance method as **dst-ip**
  - Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (for example, 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal. (CSCeh81991)

IP

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

IP Telephony

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

  No workaround is necessary. (CSCea85312)

Multicasting

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise.

  The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port.

  There is no workaround. (CSCdy82818)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

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

  There is no workaround. (CSCee16865)
- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

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

- After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

  Use one of these workarounds:

  - Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)

Quality of Service (QoS)

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue.

  The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)

- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different.

  There is no workaround. (CSCee22591)

- A QoS service policy with a policy map containing more than 62 policers cannot be added to an interface by using the **service-policy** interface configuration command.

  The workaround is to use policy maps with 62 or fewer policers. (CSCsc59418)

- 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)

SPAN and RSPAN

- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets.

  The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround. This is a hardware limitation. (CSCdy81521)

- During periods of very high traffic when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions.

  The workaround is to configure only one RSPAN source session. This is a hardware limitation. (CSCea72326)
- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session.

  The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface.

  There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y.

  There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

  There is no workaround. (CSCec35100).

VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)
- When dynamic ARP inspection is configured on a VLAN, and the ARP traffic on a port in the VLAN is within the configured rate limit, the port might go into an error-disabled state.

  The workaround is to configure the burst interval to more than 1 second. (CSCse06827)
- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

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

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)
- When the physical UID LED of the switch is on, it is blue. However, when the image of this LED on the device manager Front Panel view is on, it is green.

  There is no workaround (CSCsd98457).

Important Notes

Note Beginning with Cisco IOS Release 12.2(58)SE, the software configuration guide no longer includes a MIB appendix. 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.

- "Cisco IOS Notes" section on page 11
- "Device Manager Notes" section on page 12

Cisco IOS Notes

- The behavior of the **no logging on** global configuration command changed in Cisco IOS Release 12.2(18)SE and later. You can only use the **logging on** and then the **no logging console** global configuration commands to disable logging to the console. (CSCec71490)
- In Cisco IOS Release 12.2(25)SEC, the implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.
- 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.
- Cisco IOS Release 12.2(40)SE and later

  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)SE (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

- We recommend this browser setting to more quickly 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.
- 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** {**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 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 start 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)SE12, page 14
- Caveats Resolved in Cisco IOS Release 15.0(2)SE11, page 14
- Caveats Resolved in Cisco IOS Release 15.0(2)SE10a, page 15
- Caveats Resolved in Cisco IOS Release 15.0(2)SE10, page 15
- Caveats Resolved in Cisco IOS Release 15.0(2)SE9, page 16
- Caveats Resolved in Cisco IOS Release 15.0(2)SE8, page 16
- Caveats Resolved in Cisco IOS Release 15.0(2)SE7, page 17
- Caveats Resolved in Cisco IOS Release 15.0(2)SE6, page 18
- Caveats Resolved in Cisco IOS Release 15.0(2)SE5, page 18
- Caveats Resolved in Cisco IOS Release 15.0(2)SE4, page 19
- Caveats Resolved in Cisco IOS Release 15.0(2)SE3, page 20
- Caveats Resolved in Cisco IOS Release 15.0(2)SE1, page 21

Caveats Resolved in Cisco IOS Release 15.0(2)SE12

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/*.

Caveat ID Number	Description
CSCsv05154	Cisco IOS HTTP server vulnerable to CSRF attacks
CSCuh91645	Cisco IOS and IOS XE Software DHCP Version 4 Relay Denial of Service Vulnerability
CSCuj73916	Cisco IOS and IOS XE Software Internet Key Exchange Version 1 Denial of Service Vulnerability
CSCur29331	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCut47751	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCut50727	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCuu76493	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities
CSCvd40673	Cisco Smart Install Denial of Service Vulnerability
CSCvd72069	Test CLI Command Removal
CSCvd73487	Link Layer Discovery Protocol Buffer Overflow Vulnerability
CSCvg62730	Cisco IOS and IOS XE Software DHCP Version 4 Relay Heap Overflow Denial of Service Vulnerability
CSCvg62754	Cisco IOS and IOS XE Software DHCP Version 4 Relay Reply Denial of Service Vulnerability
CSCvg76186	Cisco Smart Install Remote Code Execution and Denial of Service Vulnerability
CSCvi05126	ISAKMP Notification messages carry unnecessary data

Caveats Resolved in Cisco IOS Release 15.0(2)SE11

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
CSCsy56638	Switch crashes after getnext on the last cafServerAliveAction index
CSCvd48893	Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability

Bug ID	Headline
CSCve60507	Crash in "mac auth bypass" SNMP code
CSCsm45390	DHCP relay security vulnerability
CSCva37748	When enable ip source guard, a part of the clients cannot communicate
CSCuw77959	1801M - %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCuz81292	IPv6 neighbor discovery packet processing behavior
CSCva74756	OSPF Rogue LSA with maximum sequence number vulnerability

Caveats Resolved in Cisco IOS Release 15.0(2)SE10a

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
CSCuu13476	Cisco IOS & IOS XE Software OpenSSH TCP Denial of Service Vulnerability
CSCuu43892	Switch crashes on qpair_full after executing dhcpd_* functions
CSCvb16274	PPTP Start-Control-Connection-Reply packet leaks router memory
CSCvb29204	BenignCertain on IOS and IOS-XE

Caveats Resolved in Cisco IOS Release 15.0(2)SE10

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
CSCum45713	UUT crashed for scale session
CSCuo95194	Switch fails while copying a configuration file to running-config using RCP
CSCus21950	Crash seen after getting LINEPROCDEAD errors and tracebacks
CSCuw71809	No warning message when switch configures "ip tcp adjust-mss"
CSCux38041	Broadcast packet does not send when port channel changes to normal port
CSCux81884	RADIUS server failover leaves port in inconsistent state
CSCuy33215	Cannot apply REP config under portchannel after initial boot up

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 a Type 5 password.

  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.

- 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.

- 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

- 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.

- 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.

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 3020 for HP and are available at Cisco.com:

http://www.cisco.com/en/US/products/ps8743/tsd_products_support_series_home.html

These documents provide complete information about the Cisco Catalyst Blade Switch 3020 for HP:

- *Cisco Catalyst Blade Switch 3020 for HP Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Blade Switch 3020 for HP*
- *Cisco Catalyst Blade Switch 3020 for HP Software Configuration Guide*
- *Cisco Catalyst Blade Switch 3020 for HP Command Reference*
- *Cisco Catalyst Blade Switch 3020 for HP System Message Guide*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.